DEGREE PROGRAMME IN WIRELESS COMMUNICATIONS ENGINEERING

MASTER'S THESIS

PHYSICAL LAYER SECURITY FOR MACHINE TYPE COMMUNICATION NETWORKS

Author	Irfan Muhammad
Supervisor	Dr. Hirley Alves
Second Examiner	Prof. Matti Latva-aho
Accepted	___ /___2018
Grade	_____

Muhammad I. (2018) Physical Layer Security for Machine Type Communication Networks. Department of Communications Engineering, University of Oulu, Oulu, Finland. Master's thesis, 48 p.

ABSTRACT

We examine the physical layer security for machine type communication networks and highlight a secure communication scenario that consists of a transmitter Alice, which employs Transmit Antenna Selection, while a legitimate receiver Bob that uses Maximum Ratio Combining, as well as an eavesdropper Eve. We provide a solution to avoid eavesdropping and provide ways to quantify security and reliability. We obtain closed-form expressions for Multiple-Input Multiple-Output and Multi-antenna Eavesdropper (MIMOME) scenario. The closed-form expressions for three useful variations of MIMOME scenario, i.e., MISOME, MIMOSE, and MISOSE are also provided. A low cost and less complex system for utilizing the spatial diversity in multiple antennas system, while guaranteeing secrecy and reliability. In our model, we assume that Bob, Alice and Eve can estimate their channel state information. We evaluate the performance of closed-form expressions in terms of secrecy outage probability and provide Monte Carlo simulations to corroborate the proposed analytical framework.

Keywords: Physical layer security, Outage probability, Reliability, Transmission rate, MIMOME, Machine type communication, TAS, MRC, Eavesdropper.

TABLE OF CONTENTS

FOREWORD

The primary focus of this thesis is to study physical layer security for machine type communication networks. This research has been financially supported by Academy of Finland 6Genesis Flagship (grant 318927) and Secure and smArt Future nEtworks (SAFE) project. First of all, I would like to thank ALLAH for his countless blessings that HE has been bestowing upon me. I would also like to express my deep sense of gratitude to my supervisor Dr. Hirley Alves for providing me an opportunity to work under his patronage. His constant support throughout this research work and his prompt responses to all my queries have made this research possible. A big thanks to Prof. Matti Latva-aho for making me a part of CWC and MTC group. I would also like to thank all members of the MTC group, where I found a chance to learn so many new things. Special thanks to Onel Luis Alcaraz López for his guidance, who despite his hectic schedule, found time to help me. I learned a lot from him.

I would like to thank my father, my siblings for their love, care and for always standing by me. I highly appreciate and thank my childhood friend Faheem Zafari who has been a great friend and no less than a brother for his support in every matter of my life whenever needed. I would also like to thank everyone from Pakistani Community in Oulu. Back home, I will also thank my friends Mr. Ali Ahmed, Mr. Ali Ahmed Aqeel, and Mr. Maqbool Elahi for their help and shared knowledge. I'm thankful to all my teachers.

I dedicate this work to my mother Ms. Shamim Akhtar (Late). Had it not been for her numerous sacrifices, her struggle, her unconditional love, her enthusiasm for knowledge, none of us (my siblings and I) would have ever made it this far. I find no words to express my feelings and love for her.

ABBREVIATIONS AND SYMBOLS

CSI	Channel State Information
MIMOME	Multiple Input Multiple Output Multiple Antenna Eavesdropper
MISOME	Multiple Input Single Output Multiple Antenna Eavesdropper
MIMOSE	Multiple Input Multiple Output Single Antenna Eavesdropper
LTE	Long Term Evolution
PDF	Probability Density Function
CDF	Cumulative Distribution Function
QoS	Quality Of Service
SNR	Signal to Noise Ratio
URLLC	Ultra Reliable Low Latency Communication
3GPP	3rd Generation Partnership Project
QoS	Quality of service
5G	Fifth mobile generation
4G	Fourth mobile generation
3G	Third mobile generation
2G	Second mobile Generation
V2V	Vehicle-to-Vehicle Communion
IoT	Internet of Things
UL	Uplink
DL	Downlink
MTC	Machine Type Communication
MTD	Machine Type Devices
HTC	Human Type Communication
eMMB	Enhanced Mobile Broadband
TAS	Transmit Antenna Selection
MRC	Maximal Ratio Combining
TTI	Transmission Time Interval
NOMA	Non-Orthogonal Multiple Access
AWGN	Additive White Gaussian Noise
PHY	Physical Layer
γ_B	Instantaneous Signal to Noise Ratio at Bob
γ_E	Instantaneous Signal to Noise Ratio at Eve
$\overline{\gamma}_B$	Average Signal to Noise Ratio at Bob
$\overline{\gamma}_E$	Average Signal to Noise Ratio at Eve
$\Gamma_{(s)}$	Gamma function
$Q\left(s,z\right)$	Regularized upper incomplete gamma function
$P\left(s,z\right)$	Regularized lower incomplete gamma function
R_S	Transmission Rate
C_b	Capacity of legitimate (Bob) link
C_e	Capacity of Eavesdropper link
$\Pr$	Probability
$\mathbb{E}[.]$	Expectation of
$\mathbf{x}_i$	transmitted signal vector of node
$\mathbf{y}_i$	received signal vector of node
$\mathbf{n}_i$	signal noise

$\mathbf{h}_i$	channel fading coefficient
$\log_e$	Natural logarithm to the base e
$\log_2$	Logarithm to the base 2

1. INTRODUCTION

The advancement in the field of wireless technologies has revolutionized the world. Nowadays, wireless networks are a vital part of our lives due to such wide-scale proliferation of wirelessly communicating devices. Both the number of devices as well as the data produced by these devices, has increased. The increase in data traffic requires enhanced capacity and bandwidth utilization, which cannot be satisfied by the existing deployed wireless technologies [1]. To fulfill these requirements, intensive research has been carried out towards the 5G of wireless communication. The technical requirements of 5G over existing deployed technologies are listed below [2];

- Thousand times higher mobile data volume per area;
- The user data rate will be ten to a hundred times higher;
- Connected number of devices will be ten to a hundred times higher than currently connected devices;
- Ten times longer battery life for low power devices;
- Low latency.

The new research led to architectural and component innovative changes in the design of 5G [3]. These changes are explained by following five technologies:

1. **Device Centric Architectures:** Cellular design depended on the self-evident role of the cell as it is the basic unit within the radio access network. Under such consideration, a device can establish downlink and uplink connection to achieve service, to carry both control and data traffic, and device location [3]. The current cell-centric architecture needs to evolve into device-centric one, where human or machine could communicate by exchanging information through various heterogeneous nodes, due to the following trends.
    - Increased data traffic caused an increase in number of users per base station (base station density) with the rise of heterogeneous networks. Some major changes in network densification are required in 5G.
    - The emerging concept of the centralized baseband is associated with cloud radio access networks [4] where virtualization is responsible for decoupling a node and hardware assigned to manage to process linked with the same node. The network operator can allocate hardware recourses to the different set of nodes dynamically.
    - Radio access network could be affected by the use of smarter devices. The architecture of both device-to-device and smart caching needs to be redefined where the center of gravity is transferred to devices, relays and wireless proxies [3]

2. **Millimeter Wave (mmWave)**: The range of millimeter wave is from 30GHz to 300GHz is high electromagnetic radiation radio frequency band known as Extremely High Frequency (EHF), while the spectrum from 3GHz to 30GHz is Super High Frequency (SHF) band. In both, SHF and EHF, the radio waves share similar propagation characteristics so the spectrum 3GHz to 300GHz with a wavelength of 1 to 100mm is referred to as millimeter Wave (mmWave) [5]. The spectrum scarcity at microwave frequencies encouraged researchers towards mmWaves and to look at various features of mmWaves transmission [3]. The mmWave frequencies have a massive amount of spectrum, i.e., local point distribution spectrum at 28-30GHz, 60GHz license-free band, E-band at 71-76 GHz, 81-86GHz and 92-95GHz [3]. The same frequency is used for mmWaves communication because of high attenuation in free space penetration, for short distances. The high frequencies of mmWave reduce antenna's physical size and enable building complex antenna arrays, which are the prominent part of mmWave. These arrays are envisioned to eradicate frequency dependence and provide maximum gain to minimize thermal noise bandwidth. Interference is brought down by narrow beam adaptive arrays, which shows the noise-limited conditions suit the mmWave system better than interference-limited conditions.

3. **Massive MIMO:** The large-scale antenna system also referred to as Massive multiple input multiple output (Massive MIMO) is the primary attribute of advanced cellular wireless systems, Massive MIMO is a multiuser MIMO, where the base station has many more antennas than devices per signaling resources [6]. The use of the law of large number averages out the frequency dependencies in the channels and hence substantial gain can be achieved. Massive MIMO provides two advantages.

   As some features are listed below [7]:

   - Spectral efficiency: The terminals' spatial multiplexing in the same time-frequency resources provides spectral efficiency. To gain efficient multiplexing, channels need to be different for different terminals sufficiently [7].
   - Energy Efficiency: The maximum array allows a reduction in radiated power and use of low-accuracy signals and linear processing save more power. [7].
   - Digital processing: Every antenna in the MIMO system has an RF and a digital baseband chain. Base station operates signals from each antenna simultaneously. The main benefit of digital processing is the uplink's channel response measurement, to nullify any assumption on the propagation channel.
   - Array gain: MIMO systems have multiple antennas, which may work in the form of an array to provide maximum gain. Gain is directly proportional to the number of the antenna in the base stations.
   - Channel hardening (a fading channel behaves as if it was a non-fading channel) eliminates the effects of fast fading. It also helps in solving resource allocation problems.

However, there is still a need to tackle research challenges in MIMO systems like channel estimation, and user mobility.

4. **Smart devices:** The previous cellular generations were designed in a way where the complete control was on the infrastructure side. This idea to be dropped in future systems. Protocol stack layers should utilize intelligence at device side, e.g., by permitting device-to-device connectivity [3].

5. **Native support for machine-to-machine communication:** Machine to machine (M2M) communication also known as Machine type communication (MTC) is an emerging technology. In M2M, a massive number of devices can be connected to a base station, unlike current systems which generally operate few hundreds of devices on a single base station. MTC communication has strong link reliability. This technology will be explained in details later.
   The aforementioned five innovative technologies could lead to both design and architectural changes in the future wireless generation. Regarding requirement and objectives, 5G has been classified into three types of communications [8], which are explained below.

1.1. Ultra-Reliable Low Latency Communication (URLLC):

Despite the enormous growth in the number of users, the commercial wireless technologies from 2G to 4G were not able to achieve 99.999% reliability. This is because the design of wireless communication technologies most of the time offer relatively good connectivity with zero data rate in those areas where coverage is quite poor with immoderate interference [8]. The communication stage where reliability is 99.999% guaranteed among devices and latency required is extremely low is known as Ultra-reliable low latency communication. URLLC is one of new operating modes in 5G and is making wireless a reliable commodity. URLLC from the perspective of supporting real-time applications with extremely low latency requirement will be used in mission-critical communication (for instance drones, virtual reality, autonomous driving, remote surgeries) [9]. URLLC has mainly two functions, latency and reliability. Latency is the time a packet takes to arrive at the receiver's physical layer from transmitter's physical layer. [10]. There are three types of latency; first, an end-to-end (E2E) latency includes queuing delay, transmission delay and computing or processing delay. Assuming latency of 1ms and considering the speed of light constraint (299,792km/s), the receiver can be located at a distance of approximately 150 km [11]. Second, a user plane latency, assuming single user, the minimum requirement is 1ms for URLLC, and the third one is control plane latency that is the time required to start a continuous data transfer from idle mode and it's minimum requirement is 20ms [11]. Reliability is the probability of successful data transmission within time period T. Reliability demands the successful data transmission under stringent latency requirements. Next, we examine the critical enablers for high reliability and low-latency communication.

1.1.1. Low-Latency

Deterministic, arbitrary or random components affect latency. The minimum latency is defined by deterministic components, with the latency's spread, mainly its tails, being affected by the arbitrary or random components. The components of deterministic latency include the time-to-transmit information, the wait-time-between-transmissions information, and the overhead (reference signals, parity bits). While on the other hand, time-to-retransmit information, overhead (when required), queuing delay, random back-off times and other computing or processing delays, comprise the random components [11]. In the following, we will discuss the different types of enablers used for low latency communication:

- **Short Transmission Time Interval (TTI), short frame structure and HARQ:** Its primary function is the reduction of TTI duration, which is achieved by utilizing fewer OFDM symbols for each TTI and by limiting OFDM symbols through broader sub-carrier spacing and by decreasing the HARQ roundtrip-time. Likewise, when the OFDM symbol duration is decreased, the sub-carrier spacing increases. Consequently, the queuing effect is accentuated due to the availability of a fewer number of resource blocks in the frequency domain. Contrary to this, control-overhead is increased, resulting in reduced capacity due to lack of resources for other URLLC data transmissions, when TTI duration is clipped. This fault is easily remedied by the use of grant-free transmission during the uplink. The downlink provides the capacity to deal with non-negligible queuing delays by using lengthier TTIs at higher loads [12].

- **eMBB/URLLC multiplexing:** Because of its latency or reliability, a static or semi-static resource between eMBB and URLLC transmissions might be preferred, but it is very inefficient when it comes to utilization of resources, and thus requires dynamic multiplexing for proper operation [12]. Instead of enhancing power of resources that are narrow-band in nature, more frequency-domain resources can be assigned to a UL (uplink) Transmission to achieve high system reliability for URLLC. It follows that wide-ranging band resources will be required for URLLC uplink transmission, if increased reliability is to be achieved while keeping latency relatively low. Likewise, whenever any new low-latency packet arrives in the middle of a frame, the routinely scheduled traffic will need to be forestalled, which can be achieved by using creative scheduling techniques. Concurrently, for maximum efficiency, the eMBB traffic should not be substantially affected if URLLC outage capacity is increased [11].

- **Edge Caching, Computing and Slicing:** Studies have shown that latency has been substantially reduced by edge computing resources and caching [13], [14]. With new technology of resource-intensive-applications (e.g., AR/VR), these trends will continue in future. Network slicing is another technology that is destined to remain in service for allocating committed resources (e.g., caching, bandwidth, computing) for services that are mission-critical.

- **On-device machine learning / Artificial intelligence (AI) on edge:** Machine Learning forms the basis for active and low-latency network systems. Conventionally the concept of ML is contingent upon only a single node (centralized).

This single node has full access to a global dataset and uses significant storage and computing capacity. Still, the inadequacies of this system for applications, which are delay sensitive and require high reliability, have warranted renewed interest in Distributed Machine Learning (e.g., Deep Learning and federated learning) which is considered the new avenue in the ubiquitous field of Artificial Intelligence, also called ML [15].

- **Grant-Free vs. Grant-Based Access:** It is either related to the dynamic scheduling of UL, or it may relate to intermittent traffic against periodic traffic with persistent scheduling. Devices operate on an optimum level when they are provided fast access to uplink on a priority basis, but this approach decreases capacity because resources are already allocated. In the same way, semi-persistent, unutilized resources can be reallocated to eMBB traffic. For collective semi-persistent scheduling, to reduce collisions, contention-based access is carried out, with the same characteristics and in the same group. Here, a base station plays a pivotal role in controlling the load and dynamically adjusting the resource pool. For optimum resource utilization, the base set makes proactive scheduling of retransmission. It does this within the same group of UE having the same traffic [16].

- **Non-Orthogonal Multiple Access (NOMA):** NOMA reduces latency, because it supports more users that are sustained by Orthogonal Multiple Access. It does so by multiplexing the domain in the uplink and then either using Successive interference cancellation (SIC) or other receivers which are more advanced such as Massage Passing, Turbo Reception. Nonetheless, issues such as user ordering, processing delay, imperfect channel state information, are not fully understood [17].

- **Low-Earth Orbit (LEO) satellites and unmanned aerial vehicles/systems:** Backhaul latency has been a big problem for long-range applications in rural areas. The use of Low-Earth Orbiting Satellites can satisfactorily resolve this problem. Moreover, the rising use of Unmanned Ariel Systems can be of great help in reducing such latencies [11].

- **Joint Flexible Resource Allocation for UL/DL:** UL/DL operating concurrently with Time Slot Length versus Switching Cost is required for TDD systems (study conducted in a context of LTE-A). LTE TDD and NR have been investigated for FDD. While only NR have been investigated for TDD because LTE TDD is not required for URLLC improvements [11].

1.1.2. Reliability

Factors affect reliability: i) channel access which is uncoordinated, that results in collision with other users; ii) the sharing of frequency by different systems; iii) interference from adjoining access channels; iv) moving devices causing Doppler shift; v) synchronization difficulty; vi) outdated CSI; vii) delayed packet reception; and viii) effects of time-varying channels. At the physical layer level, the reliability is affected by channel, constellation, error detection codes, modulation techniques, diversity, mechanisms

of retransmission. Low rate codes to induce redundancy in poor channel conditions, retransmission to correct errors and Automatic Repeat-reQuest (ARQ) in transport layers, are some methods used to increase reliability. Beamforming and diversity produce numerous independent paths, which can be used from the transmitter to receiver and can also boost the signal-to-noise ratio. The fundamental difference between frequency diversity and time diversity is that the former happens if the information is transmitted over a frequency-selective channel while the latter happens when a forward error correction codeword is distributed on various channels. Multi-user diversity, happens when transmission relaying is done by using different users right from the source to the sink [11]. In the following lines, we shall discuss various tools that facilitate reliability [11].

- **Multi-Connectivity and Harnessing Time/Frequency/RATs Diversity:** Time diversity is not always a feasible solution, especially in cases when the tolerable latency is smaller than channel coherence or in cases of stringent reliability requirements. More often than not, three-dimensional diversity is used because frequency diversity is not always on par with the number of users or devices. Therefore, high-reliable communication is most effective in enabling multi-connectivity.

- **Multicast:** Multicast is much more reliable as compared to unicast when it comes to receiving the same information. Reliability is contingent upon, the range of coverage and type of MCS used in the multicast group. The practicality of multicast is also dependent on factors such as the range of transmission (short or long) because cell edge users restrict the performance.

- **Data Replication (Contents and Computations):** Data replication is required whenever synchronization is not possible among nodes or whenever a backhaul with low-rate is needed for synchronization, or whenever there is a lack of CSI. Nevertheless, this often reduces capacity. This failure can be avoided to keep replicating the same data over and over again unless an ACK is received in case of HARQ.

- **HARQ + Short Frame Structure, Short TTI:** This is used to achieve high reliability. It does so by utilizing retransmissions to improve outage capacity. Reaching the optimum level of MCS all the while staying within the limits of reliability and latency constraints is a problem still open to research.

- **Diversity via Network Coding and Relaying:** In situations where the phenomena such as diversity of time are unreliable and extreme fading of events occurs, URLLC can only be ensured by taking care of factors such as diversity and sturdiness during the manufacturing stage. Therefore, to guarantee reliable, reciprocal communication without depending on frequency and time diversity, it is pertinent to take full advantage of network coding (using concurrent relaying) and multi-user diversity. In the same manner, not only capacity is increased by increasing the density of the network, but, latency is also reduced due to a decrease in the overall transmission range. However, it comes at the cost of backhaul provisioning. Besides, spatial diversity by using multiple antennas is a viable solution in many cases that could be exploited as in [18].

- **Network slicing:** The term Network Slicing means the slicing or splitting of a physical network into sub-networks. These sub-networks are formed in such a manner that they are optimized for specified applications, and thus ensure availability of dedicated resources for verticals, such as V2X, VR. Slicing of networks promises to be an essential tool in applications which are heterogeneous and relate to different requirements.

- **Space-Time Block Codes (STBC):** This coding technique, especially the Orthogonal STBC, is considered as a very successful transmission, diversity technique. It is because it can achieve complete diversity without invoking transmitter CSI and also does not need combined decoding of multiple symbols. Conventionally, this technique is defined by the number of free symbols (Ns) being transmitted over time slots (T). The code rate comes out to be $R_c = N_s/T$. The STBC can outperform any other similar approach, such as the Maximum Ratio Transmission technique, in case of imperfections erupt in the system.

- **Proactive Packet Drop:** If deep fade occurs, this approach helps in discarding, at the transmitter, those packets which even the maximal transmit of power cannot successfully transmit. Likewise, whenever a maximum number of retransmissions is achieved, the phenomenon of packet drop might prop-up at the receiver's end, which is different than eMBB (infinite queue buffers have been assumed here). This can be remedied by increasing the number of resources while utilizing spatial diversity.

1.2. Machine Type Communication (MTC)

MTC deals with the type of communications in which machines communicate with each other autonomously without the need for human interference, also making possible the communication with and between machines via a mobile network [19]. By the year 2020, the concept of smart cities (e.g., intercommunication and sensing capabilities between homes, vehicles, lawn mowers) will become highly mainstream. Developments in MTC and other services are destined to follow an exponential growth scale which will, in turn, give rise to many new big industries in fields such as health, entertainment, security and so forth. Advancements such as Machine-Type Deployments will also create many new types of data traffic. These traffic patterns will demand characteristics such as per-link bit rate, delay, reliability, energy, security. Current MTC depends on wireless technologies such as Bluetooth, but these work best only in short-ranges. However, for larger scale applications, wide-ranging connectivity will be required, such as 5G technologies because of Massive MTC warrants a substantial number (10 times the current number of subscribers at minimum) of connected devices. This will only be possible if the design, planning, and operation of cellular networks are transformed in the context of scalability and efficiency, to deal with diverse and dense MTD. The need for the deployment of MTC on cellular stems from the prediction that in the future a large number of devices will operate on MTC. This makes cellular networks the aptest choice, because its infrastructure, is almost universal and already in place. Low Power, Wireless LAN systems, and capillary networks will supplement MTC connectivity [20]. In summary, the phenomena of MTC over

cellular networks has become a practical reality these days. Many cellular operators around the world have already offered their subscribers the choice to subscribe to MTC [21]. Moreover, with the prediction that MTC devices will enjoy exponential growth, its benefits to the development of 5G technology have been universally recognized. Furthermore, the 3GPP has already begun working on techniques to standardize MTC over cellular [22] [23]. The only dilemma facing this technology is the timeline, i.e., when will it become a full reality, and what would be the best techniques, designs, and plans for its implementation. Certain obstacles, both technical and financial, still need to be sorted out. Although MTC can usher in a new era of economic prosperity for cellular companies, still it would not be easy to integrate the existing systems of cellular operators into MTC. A balance between the aspirations of cellular operators, auxiliary service providers, customers and regulatory bodies is pivotal to the implementation of MTC. Furthermore, the cost of implementing this system will also have to be taken into consideration. MTC can also operate by leasing cellular spectrum from spectrum owners. This makes it possible for mobile virtual network operators (MVNOs) to benefit from this technology too [20].

1.2.1. MTC Standardization in 3GPP

Technical Requirements: 3GPP radio technologies (for packet data) are in extensive usage. They can be classified in the following manner: i) from physical characteristics (GPRS using TDMA, HSPA using W-CDMA); ii) LTE systems using OFDMA. In each release of 3GPP, advancements are made to each of the above. Roaming support (key to MTC applications which require mobility support), operational capabilities across multiple platforms and backward compatibility are some of the factors behind the success of 3GPP. Since 3GPP relies on existing infrastructure, it will have a substantially low rollout cost. There is but one hiccup; 3GPP technology was designed with human interactions in mind, and not for machine interactions. They are also incompatible for MTC networks, especially greenfield developments. Some of the crucial contests facing MTC operators are terminal costs, IPR, phase-out of old technologies, terminal power consumption. Optimization of MTC for low-end applications is also a challenge due to the requirement of maintaining reverse compatibility. It is a permanent feature of mobile phones that they need regular replacement, but this shortcoming does not mar MTC devices. Furthermore, people are often averse to shifting to new technology, and making people shift to this new technology will undoubtedly be challenging [24]. With 3GPP an attempt has been made at standardizing MTC Communication. It is done by focusing on factors such as identification of particular MTC device, and large-scale adoption of MTC communication (at lower cost and increase coverage area)[24]. 3GPP has several groups: Radio access RAN, SA, FERAN, and CT. These groups describe all parameters of 3GPP technologies: interface and requirements of 3GPP systems. RAN deals with the radio access properties of 3G, 4G and so on. GERAN, on the other hand, is relatively primitive as it deals with the same for 2G. SA is used for the architecture and capabilities of the service. Lastly, CT deals with terminal interface specifications and the 3GPP systems' core areas. However, work is still in progress on 3GPP's features, and each new feature is released with a study of its core aspects [24].

The Need for MTC User Identification: An MTC module comprises two devices, a subscriber identity module (SIM) card, and an MTC device. MTC user identification is essential for most solutions offered by 3GPP. It is predicted that the SIM will have to be integrated on the PCB or have a SIM soldered directly onto the device, for most MTC subscriptions; but this requirement is not essential. In case of devices that are not integrated with the SIM, it will be the responsibility of the operator to oversee the SIM profile or the compatibility of devices. Moreover, it will have to detect any change in the device's International Mobile Equipment Identity (IMEI) in case of any misuse of the SIM card [24]. Whenever the data usage limit is reached, the identification of the particular MTC user will have to be ascertained to determine the total cost or rate of usage. Current cellular operators use a similar system of controlling the speed of mobile data as a means of reducing the price or cost of usage. The MTC system could implement a variation of the same system, but restricting mobile data may undermine the capabilities of the MTC systems because they are designed in such a way that they require the relatively larger volume of mobile data. Moreover, a user may quickly change their SIM to a non-MTC specified one, in cases where the SIM is not integrated with the device [24]. A SIM card already contains the International Mobile Subscriber Mobile (IMSI) of a subscriber which holds the subscribers' profile and the services subscribed by that person. The operators can use this information to support MTC services that are customized to each user based on their requirements of data packets size, and optimal routing. The operator holds full control of the IMSI of a user and can therefore chalk-out a pricing policy for the user, based on their preferences, with relative ease [24].

The Need for Coverage Improvement: MTC has many applications. Few of them need wide-spread coverage. Mobile MTC users will not be outside of coverage areas for longer times. However, many MTC applications require fixed terminals, but will not have fixed line access. Smart metering and vehicle parking meters are a few immobile examples of MTC applications. Those who can provide this universal connectivity will be able to claim a considerable share of the market. Nowadays, utility metering is the most apparent and in-demand application of MTC devices. Majority of establishments do not have coverage in their basements, where meters are often located, which can be remedied by adding base stations, but this comes at the cost of backhaul, acquisition of thesite and rent. Achieving of hundred percent coverage is unrealistic, but optimum coverage has to be achieved all the while keeping the cost low. Therefore, it is pertinent to ensure that the total cost of the system is not amplified while striving to improve coverage. In this connection, the 3GPP proposes improved coverage, with low intensity, of MTC modules to enable large-scale installation of MTC [21]. Study of 3GPP has identified multiple features which are redundant for MTC devices. The main focus is on reducing the complexity of devices and has identified some factors to that end, such as limiting of device competence to a single receiving RF, restriction of supported peak data rate, reduction of data bandwidth. However, this simplification gives rise to other specification impacts. It requires a fragile balance to operate this system at optimum performance, while running on standard LTE devices utilizing additional restrictions of the scheduler [24].

Service Exposure and Enablement Support: 3GPP is working to facilitate third parties to help them design third-party services to its customers, by introducing standardization. Moreover, organizations other than 3GPP are also working on standardization to enable MTC services. Support for operations such as service exposure and facilitation by 3GPP will sanction the use of 3GPP for operations other than IP-based data transmission because existing 3GPP networks already provide them, which is being done by provisioning of more information on transmission, scheduling of information, and outlining of new interfaces among 3GPP core networks and application platforms. All links with UE identity are severed by exposing network information, to ensure privacy [24] [25].

Hence, MTC adaptation is necessary for any traffic model designed for HTC. It is pertinent to ask if it would be viable to model large scale, traffic of autonomous machines, one by one, also known as source traffic modeling, which is better in terms of accuracy [26].

1.2.2. Security

A new technology, 5G (for IoT, MTC, and URLLC), has extensive use in the commercial, industrial and military sectors; it brings up several challenges. Chief among these are security and privacy problems. However, traditionally security has been seen to have limited relation with other communication tasks. Hence, the physical nature of wireless media is considered impervious to encryption algorithms [27]. Therefore, it is necessary that it ensures security and privacy of communications. However, despite these precedents, various studies (for instance [28], [29], [30] and [31]) have shown the merits of Physical Layer security as a key player in the consolidation of communication systems. In this regard, the fundamental idea promulgated by Information Theoretic Security is the combination of encryption with channel coding techniques, which helps in ensuring the security of communication, due to the communication channel's randomness, from any spying or snooping activity. We further discuss security in Chapter 2.

1.2.3. Thesis Contribution

This thesis focus on providing the solution to avoid eavesdropping and provide ways to quantify security and reliability. We study a scenario in which the transmitter Alice sends data to receiver Bob, in the existence of an experienced eavesdropper Eve, All of them are equipped with multiple antennas. Alice is perceived as a base station and Bob as a cellular user, in the context of a cellular network. Eve is operating with a slightly more complex device as compared to Bob, and resultantly might have access to private information. A low cost and less complex system for utilizing the spatial density in multiple antenna scheme, i.e., Transmit antenna selection (TAS), is employed by Alice on the main channel. Bob and Eve are utilizing an optimum Maximum Ratio Combin-

ing (MRC) scheme. Similarly, it is also assumed that Alice, Bob and Eve can estimate their own channel state information (CSI). This thesis attempts to show that in the multi-antenna environment, if a low cost and complexity single RF chain transmitter is used, the PHY security can be substantially increased, regardless of the capabilities or complexity of the eavesdroppers'receiver.

1.2.4. Thesis Outline

The rest of the thesis is organized as follows: in Chapter 2, we define a scenario where Alice (the transmitter) communicates with a Bob (the receiver) in the presence of Eve (the eavesdropper). We discuss the already derived old and new secrecy outage probability formulation for SISOSE scenario. In Chapter 3, we obtain closed-form expressions of secrecy outage probability for MISOSE, MISOME, MIMOSE and MIMOME scenarios. After that, in Chapter 4, we analyze the secrecy outage probability as a function of the rate of confidential information, average SNR of the legitimate channel and average SNR of wiretap channel. We also analyze the reliability. Finally, we present our conclusions and suggest future work in Chapter 5.

2. LITERATURE REVIEW

Currently, cryptography is utilized for security purposes and employed at upper layers of communication protocols with the assumption of eavesdropper's limited computational power: However, it is superficial and can be countered with advanced anti-cryptographic techniques/software. However, in today's world where computational power of devices grow in an exponential pattern, this technique is not viable. Furthermore, these security techniques require maintenance, distribution and constant changing of encryption codes, which is a time-consuming process and can lead to overburdening of limited resources. Lightweight cryptography and physical later security promise to be far more superior concerning achieving tight security against any level of computational power. Contemporary studies on MTC have focused upon MAC or ULA, which are used in the field such as energy management, entertainment systems. However, physical layer security has a pivotal role in MTC [32]. Since MTC communications services are defined by low power consumption, low data rate, and low mobility, this enables them to be applicable in home area networks, because of their ability for low mobility, small data transmission, group-centric communication[33]. Furthermore, physical layer security can also be used to enhance the security of location sharing and incrementing the upper-layers of security algorithms. Current Physical Layer Security Techniques have been divided into following five major categories: i) Power; ii) Theoretical Secure Capacity; iii) Code; iv) Channel and; v) Signal Detection Methods. It would be helpful to investigate as to whether the physical layer channel can assist the upper-layer security designs.

First hand, Physical Layer Security is not a novel concept, but re-merged in the recent years due to advancement in signal processing and information theory. In recent years a lot of research has been undertaken in Physical Layer Security, which has opened the possibility of new avenues in terms of designing, wireless communication networks which are are more susceptible to interception. On the other hand, due to its open nature wireless communication systems offer greater security through collaboration among different networks. The information theoretic security at the physical layer has reemerged to overcome the essential issues of cryptographic methods employed at upper layers of communication protocols, where cryptographic methods have an assumption of limited computational power at the eavesdropper [34] [35]. The drawback of cryptographic techniques is ignoring the relative location of network elements, physical properties of the wireless medium and actual transmitted information [34] [35]. Information-theoretic security compliments cryptography by adding privacy and reliability at lower layer [35]. Therefore, the design potential of Information-theoretic security can match the increasing computational powers of interceptors. Physical layer security is expected to introduce new ways to increase security and decrease the complexity of conventional cryptography as far as it is built to be protected and quantifiable (in confidential bps/Hz), in spite of the eavesdropper's computational power[35]. As making secure wireless communication system is of paramount importance, the communication system ought to have a vigilant eye on eavesdropper who tries to intercept the communication between a legitimate pair of transmitter and receiver unreliable. Due to advancement in research, the possibility to have secure communication between legitimate pair even in the presence of eavesdropper has enhanced. In 1949 Shannon introduced the concept of physical security in his pioneering work [36]. Later on, in

1975, Wyner put forward in [37] the wire-tap channel where the eavesdropper tries to breach the confidential information based on a degraded version of the legitimate link signal. They showed that there are in existence some channel codes, which can ensure error-free transmissions and discretion. It has been proved in [38] that the secrecy capacity (i.e., the maximum transmission rate at which the eavesdropper is unable to decode any information) is equal to the difference between any two channels capacities, provided that both the channels are additive white Gaussian Noise channels and the capacity of later is less than that of the former. Hence, confidential communication is possible only when the SNR of the Gaussian Main Channel is superior to the Gaussian Wiretap Channel. With the generic idea of securing wireless transmissions, in paper [27] they have focused on the effects of fading on secrecy capacity. The contributions made in [27] are: i) Information theoretic formulation for securing wireless communication; ii) secrecy capacity of single-antenna quasi-static Rayleigh fading channels, its characterization, and outage probabilities; iii) analyzing the effects of user location on secrecy; iv) detailed comparative study of a Gaussian wiretap and benefits of fading. Among other things, the most important deduction of study in [27] is that when fading is introduced still secrecy is achieved even if the eavesdropper's channel has better SNR than the main channel.

2.1. Conventional Secrecy Outage Probability

We examine the setup in Figure 2.1, where Alice is a legitimate user who sends message w to another user known as Bob. The encoded codeword $x^n = [x(1), ..., x(n)]$ of message block w is transmitted over discrete-time Rayleigh fading channel. The output of discrete-time Rayleigh fading channel (main channel) is

$$y_B(i) = h_B(i)x(i) + n_B(i),$$

Where $h_B(i)$ is the time-varying complex fading coefficient, it also refers to as channel state information (CSI) which is independent of channel output and $n_B(i)$ indicates the zero-mean circularly symmetric complex Gaussian noise. We suppose quasi-static fading where fading coefficient are constant for all channel uses i.e $h_B(i), \forall_i$.

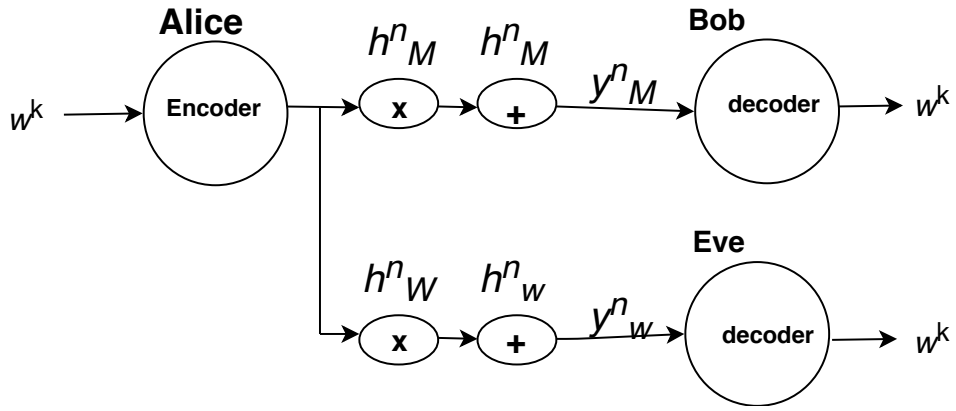

Figure 2.1: Example of wireless network with potential eavesdropper

A third party, known as Eve, who is competently eavesdropping the communication between Alice and Bob by observing an independent Rayleigh channel output

$$y_E(i) = h_E(i)x(i) + n_E(i),$$

with quasi-static fading coefficient $h_E(i) = h_E, \forall_i$ and $n_E(i)$ represents zero-mean circularly symmetric complex Gaussian noise.[27]
Note that we have power-limited channel in the sense that

$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\left[|X(i)|^2\right] \leq P$$

where P denotes average transmit signal power and $\mathbb{E}[\cdot]$ denotes expectation. Moreover main channel's noise power and wiretap channel's noise power is represented by N_B and N_E respectively. Then, The Instantaneous SNR at Bob is as follows

$$\gamma_B(i) = \frac{P|h_B(i)|^2}{N_B} = \frac{P|h_B|^2}{N_B}$$

The average SNR expression is

$$\overline{\gamma}_B(i) = \frac{P\mathbb{E}|h_B(i)|^2}{N_B} = \frac{P|h_B|^2}{N_B} = \overline{\gamma}_B$$

Similarly, the instantaneous SNR expression at Eve is given by

$$\gamma_E(i) = \frac{P|h_E(i)|^2}{N_E} = \gamma_E$$

and average SNR

$$\overline{\gamma}_E(i) = \frac{P\mathbb{E}|h_E(i)|^2}{N_E} = \overline{\gamma}_E$$

The instantaneous SNR $\gamma \propto |h|^2$ is exponentially distributed as channel fading coefficients h are zero-mean complex Gaussian random variables. Specifically, PDF of SNR at Bob and Eve are, respectively

$$p\left(\gamma_B\right) = \frac{1}{\overline{\gamma}_B}\exp\left(-\frac{\gamma_B}{\overline{\gamma}_B}\right), \gamma_B > 0 \tag{1}$$

$$p\left(\gamma_E\right) = \frac{1}{\overline{\gamma}_E}\exp\left(-\frac{\gamma_E}{\overline{\gamma}_E}\right), \gamma_E > 0 \tag{2}$$

In [27] it is assumed perfect CSI between Alice and Bob in the main channel, but no CSI between Alice and Eve. Eve, in turn, has CSI and can estimate it's own channel. Furthermore, the authors in [27] characterize the secrecy capacity of a quasi-static fading channel. Authors supposed Gaussian wiretap channel with the assumption of communication between Alice and Bob over a standard additive white Gaussian noise (AWGN) channel with noise power N_B and $N_B > N_E$, in that case, Eve's observation

is corrupted, which means Bob's receiver has better SNR than Eve's. The power is limited as $\frac{1}{n}\sum_{i=1}^{n} E[|X(i)|^2] \leqslant P$. The secrecy capacity is

$$C_s = C_B - C_E, \tag{3}$$

where C_B represents capacity of main channel while C_E indicates the capacity of Eavesdropper's channel. Their expressions are as follow.

$$C_B = \frac{1}{2}\log\left(1 + \frac{P}{N_B}\right)$$

$$C_E = \frac{1}{2}\log\left(1 + \frac{P}{N_E}\right)$$

The secrecy capacity of the wiretap channel is given as

$$C_s = \log\left(1 + \frac{P}{N_B}\right) - \log\left(1 + \frac{P}{N_E}\right),$$

per complex dimension. As h_B and h_E are quasi-static channel coefficients, then the instantaneous capacity of legitimate and eavesdropper channels are, respectively,

$$C_B = \frac{1}{2}\log\left(1 + \frac{P|h_B|^2}{N_B}\right). \tag{4}$$

$$C_E = \frac{1}{2}\log\left(1 + \frac{P|h_E|^2}{N_E}\right). \tag{5}$$

On the basis of non-negativity of channel capacity, the secrecy capacity can be written as

$$C_s = \begin{cases} \log\left(1+\gamma_B\right) - \log\left(1+\gamma_E\right) & \text{if} \gamma_B > \gamma_E \\ \\ 0 & \text{if} \gamma_B \leq \gamma_E \end{cases} \tag{6}$$

In (4) it shows that when $\gamma_B > \gamma_E$, the secrecy capacity is positive and is zero when $\gamma_B \leq \gamma_E$. As the main channel and Eavesdropper's channel are independent of each other and knowing the probability density functions given by (1), (2) of exponentially distributed random variables γ_B and γ_E, the probability of the existence of non-zero secrecy capacity can be written as [27].

$$
\begin{aligned}
\Pr\left(C_s>0\right) &\overset{(a)}{=} \Pr\left(\gamma_B>\gamma_E\right)=\int_0^{\infty}\int_0^{\gamma_B} P\left(\gamma_B,\gamma_E\right)\mathrm{d}\gamma_E\mathrm{d}\gamma_B \\
&\overset{(a)}{=} \int_0^{\infty}\int_0^{\gamma_B} P\left(\gamma_B\right)P\left(\gamma_E\right)\mathrm{d}\gamma_E\mathrm{d}\gamma_B \\
&= \int_0^{\infty}\int_0^{\gamma_B} \frac{1}{\overline{\gamma}_B}\exp\left(-\frac{\gamma_B}{\overline{\gamma}_B}\right)\frac{1}{\overline{\gamma}_E}\exp\left(-\frac{\gamma_E}{\overline{\gamma}_E}\right)\mathrm{d}\gamma_E\mathrm{d}\gamma_B \\
&= \int_0^{\infty} -\frac{1}{\overline{\gamma}_B}\exp\left(-\frac{\gamma_B}{\overline{\gamma}_B}\right)\left[\exp\left(-\frac{\gamma_B}{\overline{\gamma}_E}\right)-1\right]\mathrm{d}\gamma_B \\
&= \int_0^{\infty} -\frac{1}{\overline{\gamma}_B}\left[\exp\left(-\frac{\gamma_B}{\overline{\gamma}_B}-\frac{\gamma_B}{\overline{\gamma}_E}\right)-\exp\left(-\frac{\gamma_B}{\overline{\gamma}_B}\right)\right]\mathrm{d}\gamma_B \\
&= \int_0^{\infty} -\left[\frac{1}{\overline{\gamma}_B}+\frac{1}{\overline{\gamma}_E}\right]^{-1}\left[\exp\left(-\frac{\gamma_B}{\overline{\gamma}_B}-\frac{\gamma_B}{\overline{\gamma}_E}\right)+\overline{\gamma}_B\exp\left(-\frac{\gamma_B}{\overline{\gamma}_B}\right)\right]\mathrm{d}\gamma_B \\
&= -\frac{1}{\overline{\gamma}_B}\left[\frac{\overline{\gamma}_B\cdot\overline{\gamma}_E}{\overline{\gamma}_E+\overline{\gamma}_B}\right]-\frac{1}{\overline{\gamma}_B}\left(\overline{\gamma}_B\right) \\
&= \frac{\overline{\gamma}_B}{\overline{\gamma}_B+\overline{\gamma}_E}
\end{aligned}
\tag{7}
$$

Where (a) comes from assuming that legitimate and eavesdropper channels are independent. Notice that (7) can also be written in another way from user location point of view, where the distance between Alice and Bob is represented by d_B, and the distance between Alice and Eavesdropper by d_E. Noting that $\overline{\gamma}_B \propto d_B^{\alpha}$ and $\overline{\gamma}_E \propto d_E^{\alpha}$, α indicates the pathloss component. So the probability of the existence of non-zero secrecy capacity is given by

$$
\Pr\left(C_s>0\right)=\frac{1}{1+\left(\frac{d_B}{d_E}\right)^{\alpha}}, \tag{8}
$$

when $\gamma_B \gg \gamma_E$ or $(d_B \ll d_W)$ then $\Pr\left(C_s>0\right)\approx 1$ or $\Pr\left(C_s=0\right)\approx 0$.

Next, we are able to define the secrecy outage probability as the probability that secrecy capacity is below a target secrecy rate, thus

$$
P_{out}(R_s)=\Pr\left(C_s<R_s\right),
$$

such that the secrecy rate $R_s>0$. The operational importance of secrecy outage probability is that when setting the secrecy rate R_s Alice considers wiretap channel capacity is given by $C'_E = C_B - R_s$. Eve's channel will be worse than Alice's estimate if $R_s > C_s$, i.e., $C_E < C'_E$, Alice uses wiretap codes and these codes will provide perfect secrecy. Otherwise information secrecy is compromised if $R_s > C_s$.
In [27] authors derived the closed form equation for single input single output single eavesdropper (SISOSE) scenario, as follow

$$
P_{out}(R_s)=\Pr\left(C_s<R_s|\gamma_B>\gamma_E\right)\Pr\left(\gamma_B>\gamma_E\right)+\Pr\left(C_s<R_s|\gamma_B\leq\gamma_E\right)\Pr\left(\gamma_B\leq\gamma_E\right),
$$

where,

$$\Pr\left(\gamma_B \leq \gamma_E\right) = 1 - \Pr\left(\gamma_B > \gamma_E\right) = \frac{\overline{\gamma}_E}{\overline{\gamma}_B + \overline{\gamma}_E},$$

which comes from (7). On the other hand

$$\begin{aligned}
&\Pr\left(C_s < R_s | \gamma_B > \gamma_E\right) = \Pr\left(\log\left(1+\gamma_B\right) - \log\left(1+\gamma_E\right) < R_s | \gamma_B > \gamma_E\right), \\
&= \Pr\left(\gamma_B < 2^{R_s}\left(1+\gamma_E\right) - 1 | \gamma_B > \gamma_E\right), \\
&= \int_0^{\infty} \int_0^{2^{R_s}(1+\gamma_E)-1} \Pr\left(\gamma_B, \gamma_E | \gamma_B > \gamma_E\right) \mathrm{d}\gamma_E \mathrm{d}\gamma_B, \\
&= \int_0^{\infty} \int_0^{2^{R_s}(1+\gamma_E)-1} \frac{\Pr\left(\gamma_B\right)\Pr\left(\gamma_E\right)}{\Pr\left(\gamma_B > \gamma_E\right)} \mathrm{d}\gamma_E \mathrm{d}\gamma_B, \\
&= \int_0^{\infty} \int_0^{2^{R_s}(1+\gamma_E)-1} \frac{\frac{1}{\overline{\gamma}_B}\exp\left(-\frac{\gamma_B}{\overline{\gamma}_B}\right)\frac{1}{\overline{\gamma}_E}\exp\left(-\frac{\gamma_E}{\overline{\gamma}_E}\right)}{\frac{\overline{\gamma}_B}{\overline{\gamma}_B+\overline{\gamma}_E}} \mathrm{d}\gamma_E \mathrm{d}\gamma_B, \\
&= \frac{\overline{\gamma}_B + \overline{\gamma}_E}{\overline{\gamma}_B} . \frac{1}{\overline{\gamma}_E} \int_0^{\infty} (-1) \exp\left(-\frac{\gamma_E}{\overline{\gamma}_E} - \frac{2^{R_s}\left(1+\gamma_E\right)-1}{\overline{\gamma}_B}\right) - \exp\left(-\frac{\gamma_E}{\overline{\gamma}_E} - \frac{\gamma_E}{\overline{\gamma}_B}\right) \mathrm{d}\gamma_E, \\
&= \frac{\overline{\gamma}_B + \overline{\gamma}_E}{\overline{\gamma}_B \overline{\gamma}_E} \left[\left(\frac{\overline{\gamma}_B + 2^{R_s}\overline{\gamma}_B}{\overline{\gamma}_E \overline{\gamma}_B}\right)^{-1} \left(-\exp\left(-\frac{2^{R_s}-1}{\overline{\gamma}_B}\right)\right) + \frac{\overline{\gamma}_E . \overline{\gamma}_B}{\overline{\gamma}_E + \overline{\gamma}_B} \right] \\
&= \left[\frac{\overline{\gamma}_B + \overline{\gamma}_E}{\overline{\gamma}_B \overline{\gamma}_E} \left(\frac{\overline{\gamma}_E \overline{\gamma}_B}{\overline{\gamma}_B + 2^{R_s}\overline{\gamma}_B}\right) \left(-\exp\left(-\frac{2^{R_s}-1}{\overline{\gamma}_B}\right)\right) \right] + \left[\frac{\overline{\gamma}_E . \overline{\gamma}_B}{\overline{\gamma}_E + \overline{\gamma}_B} . \frac{\overline{\gamma}_E + \overline{\gamma}_B}{\overline{\gamma}_E . \overline{\gamma}_B} \right] \\
&= 1 - \left(\frac{\overline{\gamma}_B + \overline{\gamma}_E}{\overline{\gamma}_B + 2^{R_s}\overline{\gamma}_B}\right) \exp\left(-\frac{2^{R_s}-1}{\overline{\gamma}_B}\right)
\end{aligned} \tag{9}$$

where (a) in (9) comes from substituting (1) and (2) into (7), and since

$$R_s > 0 \implies \Pr\left(C_s < R_s | \gamma_B \leq \gamma_E\right) = 1$$

Secrecy outage for single antenna case (SISOSE) is

$$P_{out}(R_s) = 1 - \left(\frac{\overline{\gamma}_B}{\overline{\gamma}_B + 2^{R_s}\overline{\gamma}_E}\right) \exp\left(-\frac{2^{R_s}-1}{\overline{\gamma}_B}\right). \tag{10}$$

Examining the secrecy outage probability asymptotic behavior of secrecy rate R_s . If $R_s \to 0$, (10) becomes

$$P_{out}(R_s) \to \frac{\overline{\gamma}_E}{\overline{\gamma}_B + \overline{\gamma}_E}$$

and when $R_s \to \infty$ then $Pout(R_s) \to 1$, such that it's not possible for Alice and Bob to communicate secretly at very high rates. When $\overline{\gamma}_E \ll \overline{\gamma}_B$, then (10) reduces to.

$$P_{out}(R_s) = 1 - \exp\left(-\frac{2^{R_s}-1}{\overline{\gamma}_B}\right)$$

and in high SNR regime as $P_{out} \approx \left(2^{R_s}-1\right)/\overline{\gamma}_B$, otherwise when $\overline{\gamma}_B \ll \gamma_E$, $P_{out} \approx 1$, and it's impossibe for confidential communication to occur.

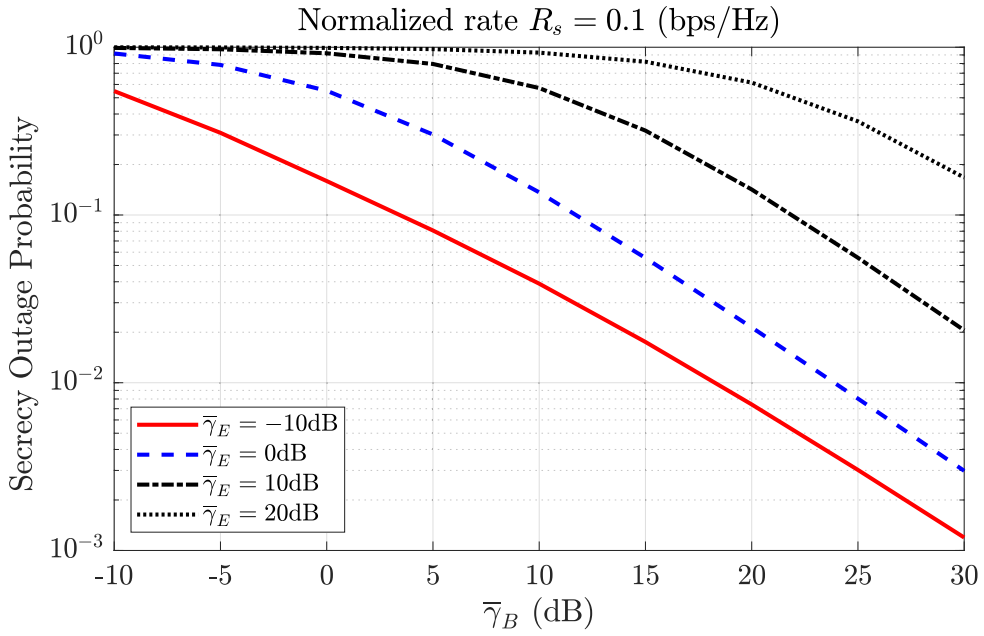

Figure 2.2: Outage probability versus $\overline{\gamma}_B$, for a normalized secrecy rate equal to 0.1 and for selected values of $\overline{\gamma}_E$. AWGN channel capacity effects Normalization with SNR equal to $\overline{\gamma}_B$

Figure 2.2 shows the secrecy outage probability versus $\overline{\gamma}_B$ for different values of $\overline{\gamma}_E$ and normalized target secrecy rate, $R_s = 0.1$. for the single antenna at all nodes. It is observed that higher $\overline{\gamma}_B$ minimizes the outage probability, and higher $\overline{\gamma}_E$ maximizes the outage probability. Furthermore the outage probability decomposes as $\frac{1}{\overline{\gamma}_B}$ if $\overline{\gamma}_B \gg \overline{\gamma}_E$. Conversely, outage probability proceed towards 1 if $\overline{\gamma}_E \gg \overline{\gamma}_B$.

Since $\overline{\gamma}_B \propto d_B^{\alpha}$ and $\overline{\gamma}_E \propto d_E^{\alpha}$, thus (11) can be written as

$$\begin{aligned} P_{out}(R_s) &= 1 - \left(\frac{\left(\frac{1}{(d_B)^{\alpha}}\right)}{\left(\frac{1}{(d_B)^{\alpha}}\right) + \left(\frac{1}{(d_E)^{\alpha}}\right) 2^{R_s}} \right) \exp\left(-\frac{2^{R_s}-1}{\overline{\gamma}_B} \right) \\ &= 1 - \left(\frac{\left(\frac{1}{(d_B)^{\alpha}}\right) (d_B)^{\alpha} (d_E)^{\alpha}}{(d_E)^{\alpha} + (d_B)^{\alpha} 2^{R_s}} \right) \exp\left(-\frac{2^{R_s}-1}{\overline{\gamma}_B} \right) \\ &= 1 - \left(\frac{1}{1 - \left(\frac{d_E}{d_B}\right)^{-\alpha} 2^{R_s}} \right) \exp\left(-\frac{2^{R_s}-1}{\overline{\gamma}_B} \right) \end{aligned} \tag{11}$$

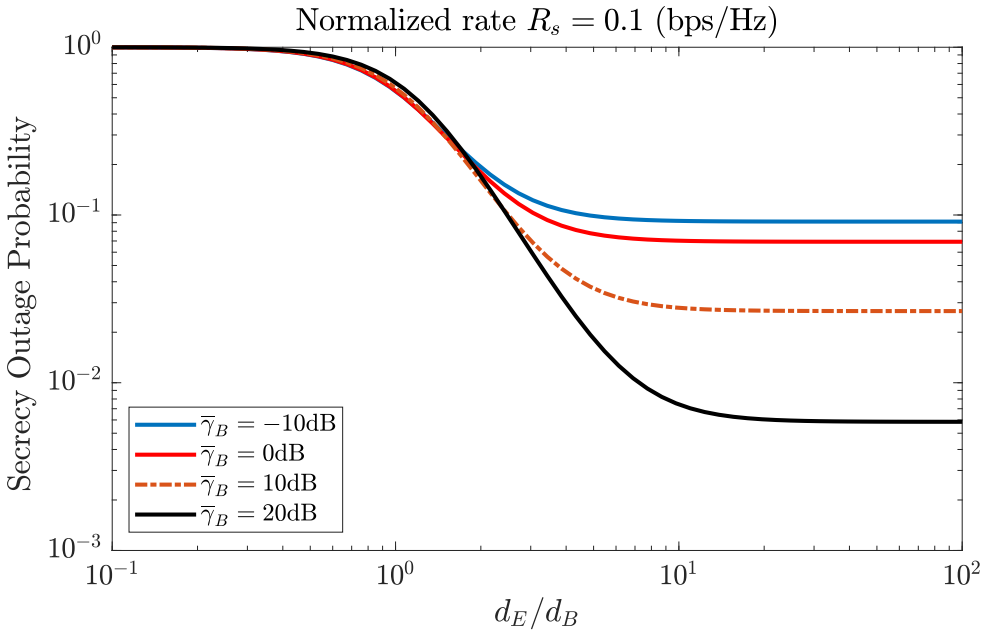

Figure 2.3: Outage probability versus d_E/d_B, for a secrecy rate equal to 0.1 and for selected values of $\overline{\gamma}_B$

In Figure 2.3, the effect of distance ratio on the performance is demonstrated for normalized target secrecy rate equal to 1 and for some selected values of $\overline{\gamma}_B$. where α = 3. When $\frac{d_E}{d_B} \to \infty$, then $P_{out}(R_s) = 1 - \exp\left(-\frac{2^{R_s}-1}{\overline{\gamma}_B}\right)$ and if $\frac{d_E}{d_B} \to 0$ then $P_{out}(R_s) = 1$. Authors in [27] disclosed that even when eavesdropper has better average SNR than the legitimate user, still perfectly secure communication over wireless channel is possible to occur.

2.2. Secrecy Outage Probability - Revised Formulation

In [39] a study of information-theoretic security has been made without any knowledge of the fading state of the eavesdropper's channel, and an alternative secrecy outage formula is presented, which is used to calculate the probability of a message transmission fails in achieving perfect secrecy. This formulation has been used to design a couple of transmission schemes which not only fulfill the required security requirements but also provide better throughput performance. The obstacle of providing information-theoretic security on wireless networks, without the information of the eavesdropper's CSI is a growing point of concern these days. Furthermore, through the provision of a probabilistic performance measure of how secure communication is, outage based characterization is the more appropriate approach. Under this context, [40] portrays an idea of secrecy outage. Closed-form expressions are presented the probability of having a secure and reliable transmission [40][41]. This formulation, however, fails to provide a direct signal of the system's security level; because, it only reads the outage events, which are not, bound to show the failures in obtaining perfect secrecy. In [39], an alternate method of formulation is presented, which provides a more thorough measure of the system's security. It does so by evaluating design parameters such as the transmission rate of code words and the circumstances in which this transmission

happens. In order to calculate the probability of how secure transmission is against eavesdropping, this formulation is better than most in terms of the framework it provides. Using this formulation two new transmission schemes have been introduced which ensure a substantial level of security and give maximum throughput. First of these schemes, needs CSI feedback from the receiver (legitimate) to the transmitter, while the other only needs 1 bit of feedback. It has been assumed that the transmission of secret information is being made from Alice to Bob on a Rayleigh fading channel, while an eavesdropper, Eve, tries to intercept the message. They have also assumed that P, the transmission power, is set to maximum. The channel gain from Alice to Bob is h_b and from Alice to Eve is h_e, Both are assumed to experience independent quasi-static fading, and receiver experiences AWGN noise. It has been assumed that both Bob and Eve have knowledge of their own channels. Nonetheless, since Alice is oblivious to Eve's instantaneous CSI, therefore complete secrecy is impossible to achieve. A substitute secrecy outage formulation for calculating the probability that a transmission has failed to achieve complete secrecy is provided in [39].

In Wyner's encoding scheme, two rates are chosen by the encoder, i.e., the rate of codewords transmitted R_b, and the rate of secret information R_s. Now, $R_e \triangleq R_b - R_s$ shows the rate of securing the transmission against eavesdropping. Bob will correctly decode the information if $C_b > R_b$; however, it will be impossible to achieve perfect secrecy if $C_e > R_e$. Therefore, the probability of secrecy outage is defined as the conditional probability [39].

$$p_{so} \triangleq P\left(C_e > R_b - R_s | message{-}transmission\right) \tag{12}$$

being conditioned on the actual transmission of the message. Their secrecy outage formulation considers design parameters as well the design parameters are taken into consideration are: transmitted codewords, and the conditions of transmission; resultantly a more stringent security metric is provided.
In [42] it is shown that whenever a transmission is successfully conducted (on the condition that Alice is oblivious to Bob's CSI) the probability of secrecy outage is turned into unconditional probability i.e. $\Pr\left(C_e > R_b - R_s\right)$. On the other hand, if Bob's Channel instantaneous CSI is available to Alice, a decision can be made by Alice regarding the sending of transmission depending on the channel condition, which has great significance because if the design of transmission condition is taken carefully, the probability of outage secrecy can be reduced substantially. This novel formulation is beneficial to the designer who can use the probability of secrecy outage to indicate the level of security and design the schemes of transmission according to the system requirements.

In [39] authors considered a scenario in which an encoder is capable of adaptively choosing the transmitted codeword rate (R_b) according to Bob's Channel instantaneous CSI. In reality, the instantaneous SNR γ_b needs to be fed from Bob to Alice. The reliability can be assessed as

$$p_{tx} = \Pr\left(\gamma_b > \mu\right) = \exp\left(-\mu/\overline{\gamma}_b\right) \tag{13}$$

Also, the secrecy outage probability closed form equation can be derived as following.

$$
\begin{aligned}
p_{so} &= \Pr\left(C_e > C_b - R_s | \gamma_b > \mu\right) \\
&= \Pr\left(\log_2\left(1+\gamma_e\right) > \log_2\left(1+\gamma_b\right) - R_s | \gamma_b > \mu\right) \\
&= \Pr\left(R_s > log_2\left(\frac{1+\gamma_b}{1+\gamma_e}\right) | \gamma_b > \mu\right) \\
&= \frac{\Pr\left(\mu < \gamma_B < 2^{R_s}\left(1+\gamma_e\right) - 1\right)}{P\left(\gamma_b > \mu\right)} \\
&= \exp\left(\frac{\mu}{\overline{\gamma}_b}\right) \int_{\frac{\mu+1}{2^{R_s}}-1}^{\infty} \int_{\mu}^{2^{R_s}(\gamma_e)-1} \Pr\left(\gamma_B\right) \Pr\left(\gamma_E\right) \mathrm{d}\gamma_E \mathrm{d}\gamma_B \\
&= \exp\left(\frac{\mu}{\overline{\gamma}_B}\right) \int_{\frac{\mu+1}{2^{R_s}}-1}^{\infty} \int_{\mu}^{2^{R_s}(\gamma_e)-1} \frac{1}{\overline{\gamma}_B} \exp\left(-\frac{\gamma_B}{\overline{\gamma}_B}\right) \frac{1}{\overline{\gamma}_e} \exp\left(-\frac{\gamma_E}{\overline{\gamma}_E}\right) \mathrm{d}\gamma_E \mathrm{d}\gamma_B \\
&= \frac{1}{\overline{\gamma}_E} \exp\left(\frac{\mu}{\overline{\gamma}_B}\right) \int_{\frac{\mu+1}{2^{R_s}}-1}^{\infty} \exp\left(-\frac{\mu}{\overline{\gamma}_E} - \frac{\gamma_E}{\overline{\gamma}_E}\right) \exp\left(-\frac{\gamma_E}{\overline{\gamma}_E} - \frac{2^{R_s}\left(1+\gamma_E\right)-1}{\overline{\gamma}_B}\right) \mathrm{d}\gamma_E \\
&= \frac{1}{\overline{\gamma}_E} \exp\left(\frac{\mu}{\overline{\gamma}_B}\right) \int_{\frac{\mu+1}{2^{R_s}}-1}^{\infty} \left[\left(\frac{-1}{\overline{\gamma}_E}\right)^{-1} \left(\frac{-1}{\overline{\gamma}_E}\right) exp\left(-\frac{\mu}{\overline{\gamma}_E} - \frac{\gamma_E}{\overline{\gamma}_E}\right)\right] \\
&- \left[\left(\frac{-2^{R_s}}{\overline{\gamma}_B} - \frac{1}{\overline{\gamma}_E}\right)^{-1} \left(\frac{-2^{R_s}}{\overline{\gamma}_B} - \frac{1}{\overline{\gamma}_E}\right) \exp\left(-\frac{\gamma_E}{\overline{\gamma}_E} - \frac{2^{R_s}\left(1+\gamma_E\right)-1}{\overline{\gamma}_B}\right)\right] \mathrm{d}\gamma_E \\
&= \frac{1}{\overline{\gamma}_E} exp\left(\frac{\mu}{\overline{\gamma}_B}\right) \left[exp\left(\frac{-\mu 2^{R_s}\overline{\gamma}_E - \overline{\gamma}_B\mu - \overline{\gamma}_B + 2^{R_s}\overline{\gamma}_B}{2^{R_s}\overline{\gamma}_E.\overline{\gamma}_B}\right)\right] \\
&\left[\frac{\overline{\gamma}_E\left(-2^{R_s}\overline{\gamma}_E - \overline{\gamma}_B\right) + \overline{\gamma}_E\overline{\gamma}_B}{-2^{R_s}\overline{\gamma}_E - \overline{\gamma}_B}\right] \\
&= \left(\frac{2^{R_s}\overline{\gamma}_E}{2^{R_s}\overline{\gamma}_E + \overline{\gamma}_B}\right) \exp\left(\frac{\mu}{\overline{\gamma}_B}\right) \left[\exp\left(\frac{-\mu 2^{R_s}\overline{\gamma}_E - \overline{\gamma}_B\mu - \overline{\gamma}_B + 2^{R_s}\overline{\gamma}_B}{2^{R_s}\overline{\gamma}_E.\overline{\gamma}_B}\right)\right] \\
&= \left(\frac{2^{R_s}\overline{\gamma}_E}{2^{R_s}\overline{\gamma}_E + \overline{\gamma}_B}\right) \left[\exp\left(\frac{-\mu\overline{\gamma}_B - \overline{\gamma}_B + 2^{R_s}\overline{\gamma}_B}{2^{R_s}\overline{\gamma}_E.\overline{\gamma}_B}\right)\right] \\
&= \left(\frac{2^{R_s}\overline{\gamma}_E}{2^{R_s}\overline{\gamma}_E + \overline{\gamma}_B}\right) \left[\exp\left(\frac{-\mu + 1 - 2^{R_s}\overline{\gamma}_B}{2^{R_s}\overline{\gamma}_E}\right)\right]
\end{aligned}
\tag{14}
$$

The new formulation in (14) is the secrecy outage probability for SISOSE scenario. Besides (13) can be used to calculate the transmission probability of any value of $R_s\left(\mu\right)$. A trade-off between Security and QoS is given by the on-off transmission's SNR threshold μ, By choosing a greater μ more stringent security can be achieved. It has been shown that P_{tx} and P_{so} are dependent on μ and R_s.

In Figure 2.4 the probability of secrecy outage is shown, by comparing the already available formulation of [27] and the newly presented formulation in (14). Both the above cases have the same rate of transmitted codewords of adaptively chosen

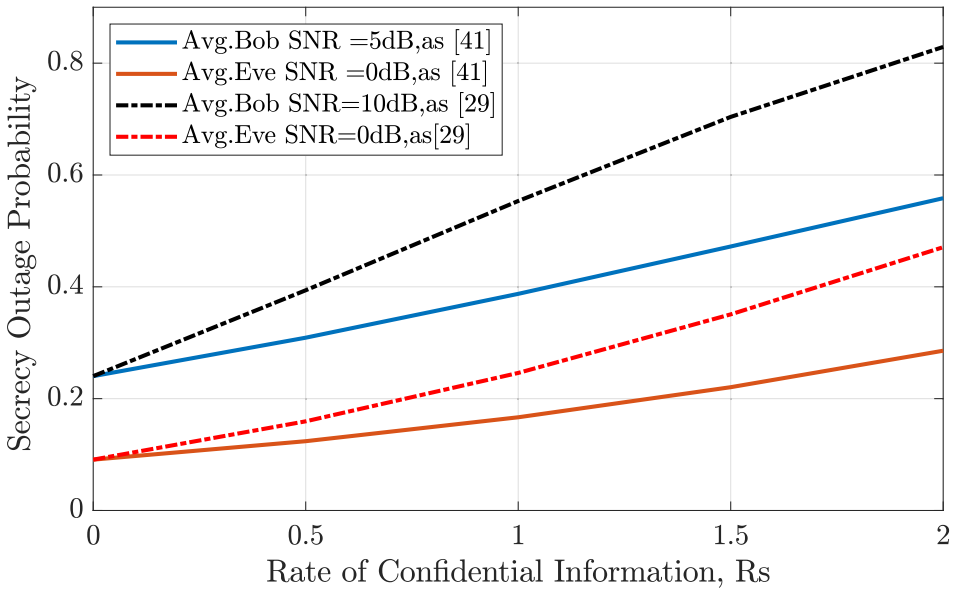

Figure 2.4: Comparison between old and new secrecy outage formulation

$R_b = C_b$. The maximum Outage probability for the new formulation is achieved by setting the on-off SNR threshold to the minimum value of $\mu = 2^{R_s - 1}$. It is clear from the figure for two different values of $\overline{\gamma}_B$ that both the formulations have noticeably different outage probabilities. Therefore, the security levels cannot be measured directly through the old formulation.

3. PERFORMANCE ANALYSIS OF TAS-MRC UNDER MULTI ANTENNA EAVESDROPPER

In this chapter, we introduce the system model and closed-form solution of a multiple antenna system operating in the presence of eavesdroppers. In chapter 2, we have revisited key metrics for performance analysis, namely secrecy outage probability, in two different formulations. Therein, we build on the top of those and provide closed-form solutions for multiple antenna system. Alice, Bob, and Eve all are able to estimate their own channel state information (CSI). Building on [43] and [44], in which a scheme is introduced that permits only Bob to benefit from transmissions of Alice, thereby reducing Eve's attack capabilities; we assume that all nodes utilize multiple antennas. However, Bob and Eve employ MRC whilst Alice performs TAS.
In our contribution, we extend the results of [44] and [39] by

- Assuming the performance of a multiple antenna wiretap channel;
- Providing generalized secrecy outage probability in closed-form;
- Providing simple closed-form expressions for the generalized secrecy outage probability of MIMOME, MIMOSE, and MISOME wiretap channels;

3.1. System Model

We consider a multiple antenna wiretap channel scenario, in which a legitimate pair communicates in the presence of an eavesdropper. Alice (the transmitter) has N_A antennas while Bob (the receiver) has N_B antennas.The untrusted, Eve (the eavesdropper), has N_E antennas and is attempting to intercept the transmission originating from Alice, as shown in Figure 3.1

The communication on the legitimate link is represented by the black line, while the red arrow shows Eve's link. However, both Bob and Alice share an open and error-free feedback channel, which is utilized to carry Alice's antenna index with optimum SNR and to allow for on-off transmission. In the case Eve obtains this feedback or knows the index of the antenna, Eve is not able to exploit such information and therefore it has no diversity gain. As legitimate and eavesdropper channels are not correlated Eve is unable to manipulate diversity from Alice's antennas.

3.1.1. Transmission Protocol and Encoding Scheme

Bob is scheduled and requests Alice to start its transmission. This request is performed through an open and error-free feedback channel, which not only carries the signaling to start the transmission but the antenna index.
The capacity of legitimate link is C_b and eavesdropper link is C_e as described in chapter 2. Subsequently, Bob selects two rates namely transmission rate R_b and confidential rate R_s. Then, the cost of securing any transmission is $R_e = R_b - R_s$ [39],[45]. Resultantly, to ensure reliability and secrecy two scenarios are presented: i) Information

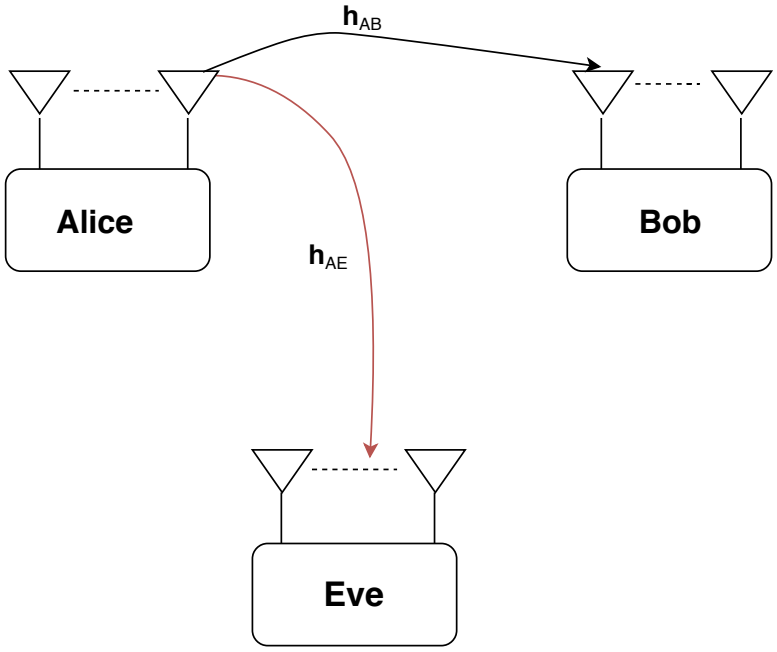

Figure 3.1: Illustrative example of network deployment: Alice utilizes TAS while Bob and Eve employ MRC, But only Bob can make use of diversity from Alice's antennas

leakage occurs if $C_e > R_e$; and ii) the message is successfully decoded at Bob whenever $C_b > R_b$ [39],[45].

3.1.2. Legitimate and Eavesdropper Channel Models

In this case, it is assumed that all channels coefficients are independent and squared-envelope is exponentially distributed. In order to get maximum SNR at Bob, a single transmit antenna is selected at Alice, and then Bob employs MRC. The best antenna's index has been defined as i^* as follow

$$i^* = \underset{1\leq\, i\, \leq N_A}{\operatorname{argmax}} ||\mathbf{h}_{iB}||, \tag{15}$$

where $N_B \times 1$ channel vector is represented by $\mathbf{h}_{iB} = [h_{i1}, h_{i2}, \cdots, h_{iN_B}]^T$ between the i-th transmit antenna at Alice and the N_B antennas at Bob with independent and identically distributed (i.i.d.) Rayleigh fading, and $||\cdot||$, $(\mathbf{x})^T$ denote the Euclidean norm and transpose operations.
Then, the message is encoded into the codeword $\mathbf{x} = [x(1, \cdots, x(i), \cdots, x(n))]$ by Alice, using the aforementioned Wyner code [46] and the transmitted codeword is bound by power constraint that $\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\left[|x(i)|^2\right] \leq P_A$, where P_A indicates transmit power of Alice, Then Bob exploits MRC to combine signal vectors, which produces the received signal at time i as follow, and $(\mathbf{x})^\dagger$ denote conjugate transpose operation.

$$y_B(i) = \mathbf{h}_{AB}^\dagger \mathbf{h}_{AB} x(i) + \mathbf{h}_{AB}^\dagger \mathbf{n}_{AB}, \tag{16}$$

where legitimate channel vector is represented by $\mathbf{h}_{AB} = \mathbf{h}_{i^*B}$, the $N_B \times 1$ additive white Gaussian noise vector at Bob is $\mathbf{n}_{AB}$, we suppose $\mathbb{E}\left[\mathbf{n}_{AB}\mathbf{n}_{AB}^{\dagger}\right] = \mathbf{I}_{N_B}\sigma_{AB}^2$, with σ_{AB}^2 being the noise variance at each antenna, while $\mathbf{I}_{N_B}$ is a $m \times m$ identity matrix. Thus, the instantaneous SNR of the legitimate link from (16) is

$$\gamma_B = \frac{||\mathbf{h}_{AB}||^2 P_A}{\sigma_{AB}^2}, \tag{17}$$

Probability density function (PDF) and cumulative distribution function (CDF) of a given random variable X are denoted as $f_X(x)$ and $F_X(x)$, respectively, as in [47]

$$f_{\gamma_B}(\gamma) = \frac{N_A\, \gamma^{N_B-1}}{\Gamma(N_B)\, \overline{\gamma}_B^{N_E}} \exp\left(-\frac{\gamma}{\overline{\gamma}_B}\right) \mathrm{P}\left(N_B\,,\, \frac{\gamma}{\overline{\gamma}_B}\right)^{N_A-1}, \tag{18}$$

$$F_{\gamma_B}(\gamma) = \mathrm{P}\left(N_B\,,\, \frac{\gamma}{\overline{\gamma}_B}\right)^{N_A}. \tag{19}$$

It is clear from (18) and (19) that diversity of Alice's and Bob's numerous antennas is exploited by the legitimate channel. While Eve can only utilize its own antenna's diversity because it perceives a random TAS scheme. As a result, the eavesdropped signal vector using MRC is combined by Eve at time i : as follow

$$y_E(i) = \mathbf{h}_{AB}^{\dagger}\mathbf{h}_{AE}x(i) + \mathbf{h}_{AE}^{\dagger}\mathbf{n}_{AE}, \tag{20}$$

where eavesdropper channel vector is represented by $\mathbf{h}_{AE} = \mathbf{h}_{i^*E}$, the $N_E \times 1$ additive white Gaussian noise vector at Eve is $\mathbf{n}_{AE}$, we suppose $\mathbb{E}\left[\mathbf{n}_{AE}\mathbf{n}_{AE}^{\dagger}\right] = \mathbf{I}_{N_E}\sigma_{AE}^2$, with σ_{AE}^2 being the noise variance at each antenna. All channels undergo Rayleigh fading, likewise to the legitimate link. Thus, the instantaneous SNR of the eavesdropper link from (20) is

$$\gamma_E = \frac{||\mathbf{h}_{AE}||^2 P_A}{\sigma_{AE}^2}, \tag{21}$$

which follows Gamma distribution, and its PDF and CDF are given respectively as [47]

$$f_{\gamma_E}(\gamma) = \frac{\gamma^{N_E-1}}{\Gamma(N_E)\, \overline{\gamma}_E^{N_E}} \exp\left(-\frac{\gamma}{\overline{\gamma}_E}\right), \tag{22}$$

$$F_{\gamma_E}(\gamma) = \mathrm{P}\left(N_E\,,\, \frac{\gamma}{\overline{\gamma}_E}\right) \tag{23}$$

3.2. Secrecy Outage Probability

It is clear from the above discussion that two basic conditions can be manipulated to ensure reliability and security [39], [46]. In the context of reliability, the channel capacity has to be higher than the transmission rate. Hence, $C_b > R_b$, which ensures

that the message is decoded. Therefore, the probability of successful transmissions for this scheme is defined as

$$\begin{aligned} p_s(\mu) &= \Pr\left[C_b > R_b\right] = \Pr\left[\gamma_B > \mu\right] \\ &= 1 - F_{\gamma_B}(\mu) \end{aligned} \tag{24}$$

where $F_{\gamma_B}(\cdot)$ is given in (19) and $\mu \geq 2^{R_s} - 1$ because a transmission only occurs when $C_b > R_s$. We resort to a secrecy outage probability metric introduced in [39], which is conditioned on a successful transmission at the legitimate channel. Thus, the secrecy outage is defined as

$$p_{so} \stackrel{\triangle}{=} \Pr\left[C_e > C_b - R_s | \gamma_B > \mu\right], \tag{25}$$

$$= \frac{\Pr\left[\mu < \gamma_B < 2^{R_s}(1+\gamma_E) - 1\right]}{p_s(\mu)} \tag{26}$$

$$\begin{aligned} &= \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \frac{F_{\gamma_B}\left(2^{R_s}(1+\gamma_E) - 1\right) f_{\gamma_E}(\gamma_E)\mathrm{d}\gamma_E}{1 - F_{\gamma_B}(\mu)} \\ &\quad - \frac{\left(1 - F_{\gamma_E}\left(\frac{(1+\mu)}{2^{R_s}} - 1\right)\right) F_{\gamma_B}(\mu)}{1 - F_{\gamma_B}(\mu)}, \end{aligned} \tag{27}$$

where (27) holds when assuming independent random variables.

3.2.1. Generalized MIMOME Scenario

In this section, we get the closed-form expression of secrecy outage probability for MIMOME scenario. We solve (27) with respect to instantaneous SNR γ_E at Eve. Where the term on the right hand side of (27) becomes

$$\frac{\left(1 - F_{\gamma_E}\left(\frac{(1+\mu)}{2^{R_s}} - 1\right)\right) F_{\gamma_B}(\mu)}{1 - F_{\gamma_B}(\mu)} = \frac{1}{p_s(\mu)} Q\left(N_E, -\frac{2^{R_s} - 1 - \mu}{2^{R_s}\overline{\gamma}_E}\right) P\left(N_B, \frac{\mu}{\overline{\gamma}_B}\right)^{N_A}. \tag{28}$$

Gamma function is defined as $\Gamma(z)$[48 ,Ch 6, 6.1.1], while the regularized lower incomplete gamma function is denoted as $\mathrm{P}(s,z) = \frac{\gamma(s,z)}{\Gamma(z)}$ [48 ,Ch 6, 6.5.1] and regularized upper incomplete gamma function is denoted as $\mathrm{Q}(s,z) = \frac{\gamma(s,z)}{\Gamma(z)}$ [48 ,Ch 26.4, 26.4.19]
Then, the integral in (27) can be defined as

$$I = \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \frac{F_{\gamma_B}\left(2^{R_s}(1+\gamma_E) - 1\right) f_{\gamma_E}(\gamma_E)\mathrm{d}\gamma_E}{1 - F_{\gamma_B}(\mu)} \tag{29}$$

$$\overset{(a)}{=} \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} P\left(N_B, \frac{(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right)^{N_A} \frac{\gamma_E^{N_E-1}}{\Gamma(N_E)\,\overline{\gamma}_E^{N_E}} \exp\left(\frac{-\gamma_E}{\overline{\gamma}_E}\right) \mathrm{d}\gamma_E$$

$$\overset{(b)}{=} \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \left(\frac{\Gamma(N_B) - \Gamma(N_B)\exp\left(-\frac{(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right)\sum_{k=0}^{N_B-1}\left(\frac{(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right)^k \frac{1}{k!}}{\Gamma(N_B)}\right)^{N_A}$$

$$\frac{\gamma_E^{N_E-1}}{\Gamma(N_E)\,\overline{\gamma}_E^{N_E}} \exp\left(\frac{-\gamma_E}{\overline{\gamma}_E}\right) \mathrm{d}\gamma_E,$$

$$\overset{(c)}{=} \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \left(1 - \exp\left(-\frac{(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right)\sum_{t=0}^{N_B-1}\left(\frac{(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right)^t \frac{1}{t!}\right)^{N_A}$$

$$\frac{\gamma_E^{N_E-1}}{\Gamma(N_E)\,\overline{\gamma}_E^{N_E}} \exp\left(\frac{-\gamma_E}{\overline{\gamma}_E}\right) \mathrm{d}\gamma_E,$$

Where (a) comes after replacing (19) and (22) into (29), then with the help of [48 ,Ch 6, 6.5.1] we write (b), and after further simplification, we attain (c). Next, after applying binomial expansion in (c) we attain (d)

$$\overset{(d)}{=} \sum_{K=0}^{N_A} \binom{N_A}{K} (-1)^K \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \exp\left(-\frac{(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right)^K$$

$$\left(\sum_{t=0}^{N_B-1}\left(\frac{(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right)^t \frac{1}{t!}\right)^K \frac{\gamma_E^{N_E-1}}{\Gamma(N_E)\,\overline{\gamma}_E^{N_E}} \exp\left(\frac{-\gamma_E}{\overline{\gamma}_E}\right) \mathrm{d}\gamma_E$$

$$\overset{(e)}{=} \sum_{K=0}^{N_A} \binom{N_A}{K} (-1)^K \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \exp\left(-\frac{(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right)^K$$

$$\left(1 + \frac{1}{1!}\left(\frac{(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right)^1 + ... + \frac{1}{(N_B-1)!}\left(\frac{(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right)^{N_B-1}\right)^K$$

$$\frac{\gamma_E^{N_E-1}}{\Gamma(N_E)\,\overline{\gamma}_E^{N_E}} \exp\left(\frac{-\gamma_E}{\overline{\gamma}_E}\right) \mathrm{d}\gamma_E$$

$$\overset{(f)}{=} \sum_{K=0}^{N_A} \binom{N_A}{K} (-1)^K \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \exp\left(-\frac{K(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right)$$

$$\sum_{s_0+s_1+s_2+..s_{N_B-1}=K} \binom{K}{s_0, s_1, s_2, .., s_{N_B-1}} \prod_{t=0}^{N_B-1}\left(\frac{1}{t!}\right)^{s_t}\left(\frac{(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right)^{s_t * t}$$

$$\frac{\gamma_E^{N_E-1}}{\Gamma(N_E)\,\overline{\gamma}_E^{N_E}} \exp\left(\frac{-\gamma_E}{\overline{\gamma}_E}\right) \mathrm{d}\gamma_E$$

Note that in (e) we expand the inner summation and in (f) we apply multinomial theorem. Next, we simplify (f) and apply the binomial expansion into $\left(\frac{(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right)^{s_t*t}$ as follows

$$\overset{(g)}{=} \sum_{K=0}^{N_A} \binom{N_A}{K} (-1)^K \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \exp\left(-\frac{K(2^{R_s}-1)}{\overline{\gamma}_B}\right) \exp\left(-\frac{K(2^{R_s}\gamma_E)}{\overline{\gamma}_B}\right)$$
$$\sum_{s_0+s_1+s_2+..+s_{N_B-1}=K} \binom{K}{s_0, s_1, s_2, .., s_{N_B-1}} \prod_{t=0}^{N_B-1} \left(\frac{1}{t!}\right)^{s_t} \left(\left(\frac{2^{R_s}-1}{\overline{\gamma}_B}\right) + \left(\frac{2^{R_s}\gamma_E}{\overline{\gamma}_B}\right)\right)^{s_t*t}$$
$$\frac{\gamma_E^{N_E-1}}{\Gamma(N_E)\,\overline{\gamma}_E^{N_E}} \exp\left(\frac{-\gamma_E}{\overline{\gamma}_E}\right) \mathrm{d}\gamma_E$$
$$\overset{(h)}{=} \sum_{K=0}^{N_A} \binom{N_A}{K} (-1)^K \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \exp\left(-\frac{K(2^{R_s}-1)}{\overline{\gamma}_B}\right) \exp\left(-\frac{K(2^{R_s}\gamma_E)}{\overline{\gamma}_B}\right)$$
$$\sum_{s_0+s_1+..+s_{N_B-1}=K} \binom{K}{s_0, s_1, .., s_{N_B-1}} \prod_{t=0}^{N_B-1} \left(\frac{1}{t!}\right)^{s_t} \sum_{p=0}^{s_t*t} \binom{s_t*t}{p} \left(\frac{2^{R_s}-1}{\overline{\gamma}_B}\right)^{s_t*t-p} \left(\frac{2^{R_s}\gamma_E}{\overline{\gamma}_B}\right)^{p}$$
$$\frac{\gamma_E^{N_E-1}}{\Gamma(N_E)\,\overline{\gamma}_E^{N_E}} \exp\left(\frac{-\gamma_E}{\overline{\gamma}_E}\right) \mathrm{d}\gamma_E$$

And after some simplification, we obtain

$$\overset{(i)}{=} \sum_{K=0}^{N_A} \binom{N_A}{K} (-1)^K \exp\left(-\frac{K(2^{R_s}-1)}{\overline{\gamma}_B}\right) \sum_{s_0+s_1+..s_{N_B-1}=K} \binom{K}{s_0, s_1, .., s_{N_B-1}}$$
$$\prod_{t=0}^{N_B-1} \left(\frac{1}{t!}\right)^{s_t} \sum_{p=0}^{s_t*t} \binom{s_t*t}{p} \left(\frac{2^{R_s}-1}{\overline{\gamma}_B}\right)^{s_t*t-p} \frac{1}{\Gamma(N_E)\,\overline{\gamma}_E^{N_E}}$$
$$\int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \exp\left(-\frac{K(2^{R_s}\gamma_E)}{\overline{\gamma}_B}\right) \left(\frac{2^{R_s}}{\overline{\gamma}_B}\right)^{p} (\gamma_E)^p\, \gamma_E^{N_E-1} \exp\left(\frac{-\gamma_E}{\overline{\gamma}_E}\right) \mathrm{d}\gamma_E \tag{30}$$

Finally thus last integral is solved as follows

$$\begin{aligned} I_2 &= \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \exp\left(-\frac{K(2^{R_s}\gamma_E)}{\overline{\gamma}_B}\right) \left(\frac{2^{R_s}}{\overline{\gamma}_B}\right)^{p} (\gamma_E)^p\, \gamma_E^{N_E-1} \exp\left(\frac{-\gamma_E}{\overline{\gamma}_E}\right) \mathrm{d}\gamma_E \\ &= \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \gamma_E^{p+N_E-1} \exp\left(-\frac{K(2^{R_s}\gamma_E)}{\overline{\gamma}_B} - \frac{\gamma_E}{\overline{\gamma}_E}\right) \mathrm{d}\gamma_E \\ &= \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \gamma_E^{p+N_E-1} \exp\left(\frac{-\gamma_E\left(K2^{R_s}\overline{\gamma}_E + \overline{\gamma}_B\right)}{\overline{\gamma}_E\overline{\gamma}_B}\right) \mathrm{d}\gamma_E \\ &= \left(\frac{K2^{R_s}\overline{\gamma}_E + \overline{\gamma}_B}{\overline{\gamma}_B\overline{\gamma}_E}\right)^{-p-N_E} \Gamma\left[(p+N_E), \left(\frac{K2^{R_s}\overline{\gamma}_E + \overline{\gamma}_B}{\overline{\gamma}_B\overline{\gamma}_E}\right)\left(\frac{\mu+1-2^{R_s}}{-2^{R_s}\overline{\gamma}_E}\right)\right] \end{aligned} \tag{31}$$

By substituting (31) into (30), and putting (30), (24) and (28) into (27) we attain the closed form of secrecy outage probability of the MIMOME wiretap channel, where Alice employs TAS while Bob and Eve perform MRC.

$$
\begin{aligned}
p_{so} = & \sum_{K=0}^{N_A} \binom{N_A}{K} \frac{(-1)^K}{1-p_s(\mu)} \exp\left(-\frac{K(2^{R_s}-1)}{\overline{\gamma}_B}\right) \sum_{s_0+s_1+..s_{N_B-1}=K} \binom{K}{s_0, s_1, .., s_{N_B-1}} \\
& \prod_{t=0}^{N_B-1} \left(\frac{1}{t!}\right)^{s_t} \sum_{p=0}^{s_t*t} \binom{s_t*t}{p} \left(\frac{2^{R_s}-1}{\overline{\gamma}_B}\right)^{s_t*t-p} \left(\frac{2^{R_s}}{\overline{\gamma}_B}\right)^{p} \frac{1}{\Gamma(N_E)\,\overline{\gamma}_E^{N_E}} \\
& \left(\frac{K2^{R_s}\overline{\gamma}_E+\overline{\gamma}_B}{\overline{\gamma}_B\overline{\gamma}_E}\right)^{-p-N_E} \Gamma\left[(p+N_E), \left(\frac{K2^{R_s}\overline{\gamma}_E+\overline{\gamma}_B}{\overline{\gamma}_B\overline{\gamma}_E}\right)\left(\frac{\mu+1-2^{R_s}}{-2^{R_s}\overline{\gamma}_E}\right)\right] \\
& - \frac{1}{p_s(\mu)} Q\left(N_E, -\frac{2^{R_s}-1-\mu}{2^{R_s}\overline{\gamma}_E}\right) P\left(N_B, \frac{\mu}{\overline{\gamma}_B}\right)^{N_A}
\end{aligned} \tag{32}
$$

3.2.2. MISOME Scenario

For MISOME scenario, Bob is a single antenna device; thus the only source of spatial diversity in the legitimate link comes from Alice antennas. Next, we evaluate three useful variations of the MIMOME scenario, for which we provide a simpler closed-solution. Taking (27) into account and simplifying (19) for $N_B = 1$ we have

$$
\begin{aligned}
I &= \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} P\left(N_B, \frac{(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right)^{N_A} \frac{\gamma_E^{N_E-1}}{\Gamma(N_E)\,\overline{\gamma}_E^{N_E}} \exp\left(\frac{-\gamma_E}{\overline{\gamma}_E}\right) \mathrm{d}\gamma_E \\
&= \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \left(1-\exp\left(-\frac{(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right)\right)^{N_A} \frac{\gamma_E^{N_E-1}}{\Gamma(N_E)\,\overline{\gamma}_E^{N_E}} \exp\left(\frac{-\gamma_E}{\overline{\gamma}_E}\right) \mathrm{d}\gamma_E
\end{aligned}
$$

Then, we apply binomial theorem on $\left(1-\exp\left(-\frac{(2^{R_s}(1+\gamma_E)-1}{\overline{\gamma}_B}\right)\right)^{N_A}$ and simplify it such that

$$
\begin{aligned}
I = & \sum_{K=0}^{N_A} \binom{N_A}{K} (-1)^K \exp\left(-\frac{K(2^{R_s}-1)}{\overline{\gamma}_B}\right) \int_{\frac{(1+\mu)}{2^{R_s}}-1}^{\infty} \exp\left(-\frac{K(2^{R_s}\gamma_E)}{\overline{\gamma}_B}\right) \\
& \frac{\gamma_E^{N_E-1}}{\Gamma(N_E)\,\overline{\gamma}_E^{N_E}} \exp\left(\frac{-\gamma_E}{\overline{\gamma}_E}\right) \mathrm{d}\gamma_E
\end{aligned} \tag{33}
$$

we obtain secrecy outage probability for MISOME scenario where Alice employs TAS while Eve performs MRC in (34) after substituting (24),(33) into (27), thus the closed-form expression for MISOME scenario is

$$p_{so}=\sum_{k=0}^{N_A}\binom{N_A}{k}\frac{(-1)^k}{p_s(\mu)}\exp\left(-k\frac{2^{R_s}-1}{\overline{\gamma}_B}\right)\left(\frac{\overline{\gamma}_B}{\overline{\gamma}_B+k2^{R_s}\overline{\gamma}_E}\right)^{N_E}$$
$$\mathrm{Q}\left(N_E,-\frac{\left(\overline{\gamma}_B+k2^{R_s}\overline{\gamma}_E\right)\left(2^{R_s}-1-\mu\right)}{2^{R_s}\overline{\gamma}_B\overline{\gamma}_E}\right)$$
$$-\frac{1}{p_s(\mu)}\left(1-\exp\left(-\frac{\mu}{\overline{\gamma}_B}\right)\right)^{N_A}\mathrm{Q}\left(N_E,-\frac{2^{R_s}-1-\mu}{2^{R_s}\overline{\gamma}_E}\right). \quad (34)$$

3.2.3. MISOSE Scenario

The closed-form expression for secrecy outage probability of the MISOSE wiretap channel, where only Alice has multiple antennas and then employs TAS, is given as

$$p_{so}=\exp\left(\frac{2^{R_s}-1-\mu}{2^{R_s}\overline{\gamma}_E}\right)\left[{}_2\mathrm{F}_1\left(-N_A,\frac{\overline{\gamma}_B}{2^{R_s}\overline{\gamma}_E},1+\frac{\overline{\gamma}_B}{2^{R_s}\overline{\gamma}_E},e^{-\frac{\mu}{\overline{\gamma}_B}}\right)\right.$$
$$\left.-\left(1-\exp\left(-\frac{\mu}{\overline{\gamma}_B}\right)\right)^{N_A}\right]\frac{1}{p_s(\mu)}. \quad (35)$$

3.2.4. MIMOSE Scenario

Secrecy outage probability of the MIMOSE wiretap channel where Alice and Bob, both have multiple antennas but Eve is a single antenna device. Alice employs TAS and Bob resorts MRC.

$$p_{so}=\sum_{K=0}^{N_A}\binom{N_A}{K}\frac{(-1)^K}{1-p_s(\mu)}\exp\left(-\frac{K(2^{R_s}-1)}{\overline{\gamma}_B}\right)\sum_{s_0+s_1+..s_{N_B-1}=K}\binom{K}{s_0,s_1,..,s_{N_B-1}}$$
$$\prod_{t=0}^{N_B-1}\left(\frac{1}{t!}\right)^{s_t}\sum_{p=0}^{s_t*t}\binom{s_t*t}{p}\left(\frac{2^{R_s}-1}{\overline{\gamma}_B}\right)^{s_t*t-p}\left(\frac{2^{R_s}}{\overline{\gamma}_B}\right)^{p}\left(\frac{K2^{R_s}\overline{\gamma}_E+\overline{\gamma}_B}{\overline{\gamma}_B\overline{\gamma}_E}\right)^{-p-1}$$
$$\Gamma\left[(p+1),\left(\frac{K2^{R_s}\overline{\gamma}_E+\overline{\gamma}_B}{\overline{\gamma}_B\overline{\gamma}_E}\right)\left(\frac{\mu+1-2^{R_s}}{-2^{R_s}\overline{\gamma}_E}\right)\right]-\frac{1}{p_s(\mu)}Q\left(N_E,-\frac{2^{R_s}-1-\mu}{2^{R_s}\overline{\gamma}_E}\right)$$
$$P\left(N_B,\frac{\mu}{\overline{\gamma}_B}\right)^{N_A} \quad (36)$$

4. NUMERICAL ANALYSIS

In the previous chapter, we derived the closed-form expressions of secrecy outage probabilities for MIMOME, MIMOSE, MISOME and MISOSO scenarios. In this chapter, we discuss the numerical analysis of these expressions as a function of average SNR at Bob $\overline{\gamma}_B$, average SNR at Eve $\overline{\gamma}_E$ and rate of confidential information R_S. We analyze the impact of these parameters on secrecy outage probability with the different combination of the antennas at Alice, Bob and Eve. We also analyze the reliability of communication.

4.1. Comparison Between Conventional and Revisited Formulation

We compare the conventional and revisited secrecy outage formulation for MISOME scenario. The old secrecy outage formulation for MISOME is given in [44] and an

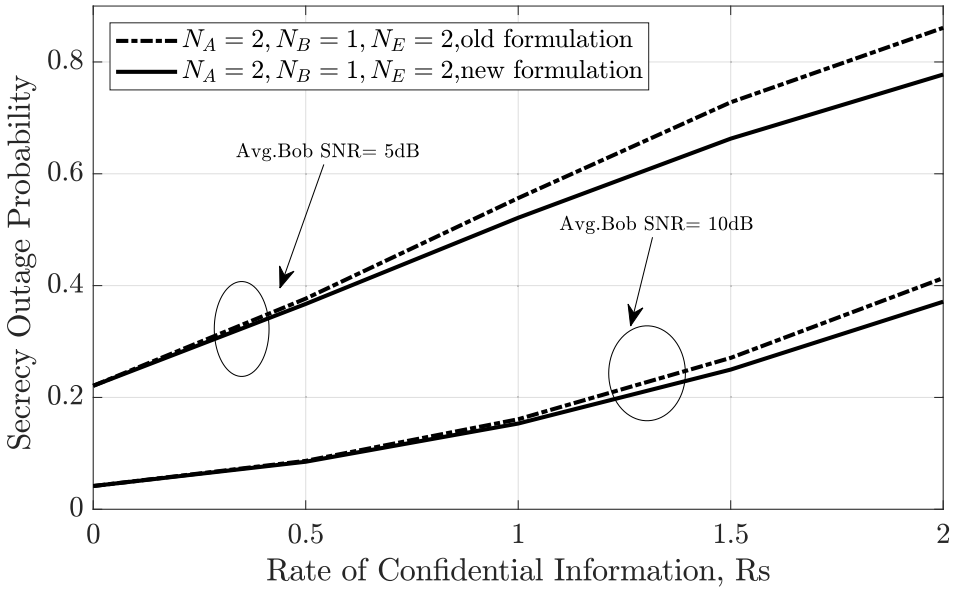

Figure 4.1: Secrecy outage probability versus Rs for MISOME scenario

alternative secrecy outage formula is presented in (36), which is used to calculate the probability of a message transmission not achieving perfect secrecy. This formulation will be used to fulfill the required security requirements. Figure 4.1 shows the secrecy outage probability as a function of the rate of confidential information. We present the comparison between old secrecy outage formulation given in [44] and new secrecy outage formulation given in (36) for MISOME scenario for two antennas at Alice, single at Bob and two at Eve. Alice can be treated as a base station in a network while Bob as a mobile user. Where Alice employs, transmit antenna selection scheme and Eve resorts to the maximum ratio combining. The new formulation has the rate of transmitted codewords adaptively chosen as $R_b = C_b$. For different values of rate of confidential information, the maximum outage probability for the new formulation is achieved by setting the on-off SNR threshold to the minimum value of $\mu = 2^{R_s - 1}$. The average SNR at Eve, $\overline{\gamma}_E$ is 0 dB. It is clear from the figure for two different val-

ues of average SNR at Bob $\overline{\gamma}_B$ that both formulations have noticeably different outage probabilities. We observe from the Figure 4.1 that secrecy outage is reduced in the new formulation. Therefore, the security levels cannot be measured directly through the old formulation anymore. Simulation results show security can be improved with an increase in the number of Alice's antenna, even if Eve has multiple antennas. Our proposed TAS scheme requires only one RF chain, resulting in a reduced cost, power consumption, operation complexity and size at the cost of a small loss in performance when compared with multiple RF chains.

4.2. Impact of the Number of Antennas on Secrecy Performance

In this section, we analyze the impact of number of antennas on secrecy performance for MISOSE and MIMOME scenario as a function of legitimate link SNR and confidential rate.

4.2.1. MISOSE Scenario

Figure 4.2 shows the secrecy outage probability of SISOSE and MISOSE scenarios as a function of confidential rate. In SISOSE case, Alice, Bob and Eve are single nodes. Let's assume that Alice can access the CSI on both main and Eve's channel. This is primarily the case in Time Division Multiple Access (TDMA) setting where Eve is not necessarily an eavesdropper but another user or node. Alice can estimate the CSI on both the channels by sending communication signals. Alice can leverage the available CSI on both channels for achieving the required secrecy through the transmission of useful symbols to Bob when the instantaneous SNR values are such that the instanta-

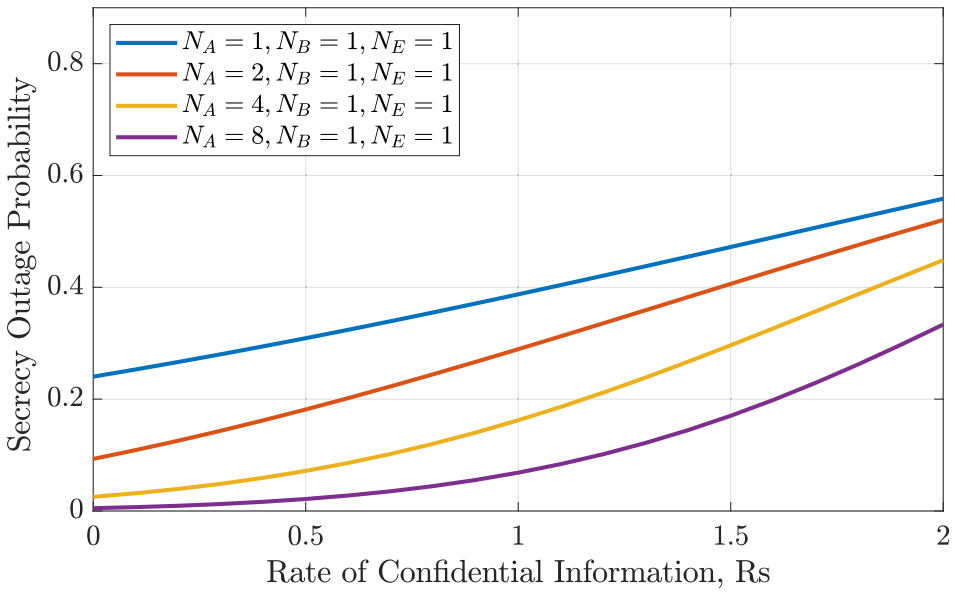

Figure 4.2: Secrecy outage probability versus Confidential rate

neous secrecy capacity is strictly positive ($\gamma_B > \gamma_E$), which allows achieving a certain degree of confidentiality even in the case where the eavesdropper's channel is better than the main channel. There is great gain in reliability with an increased number of the antenna at the transmitter as compared to SISOSE scenario. In MISOSE case only Alice has multiple antennas to apply TAS scheme for transmission. For $\overline{\gamma}_B$ = 5 dB and $\overline{\gamma}_E$= 0 dB, we compare secrecy outage probability for different number of transmit antennas. We can notice from the figure 4.2 that with the increasing number of transmit antennas, the secrecy outage probability decreases for SISOSE and MISOSE scenarios.

4.2.2. MIMOME Scenario

The secrecy performance of MIMOME scenario is discussed for different setup of antennas. In Figure 4.3, for an eavesdropper channel with average SNR, $\bar{\gamma}_E = 0$dB and

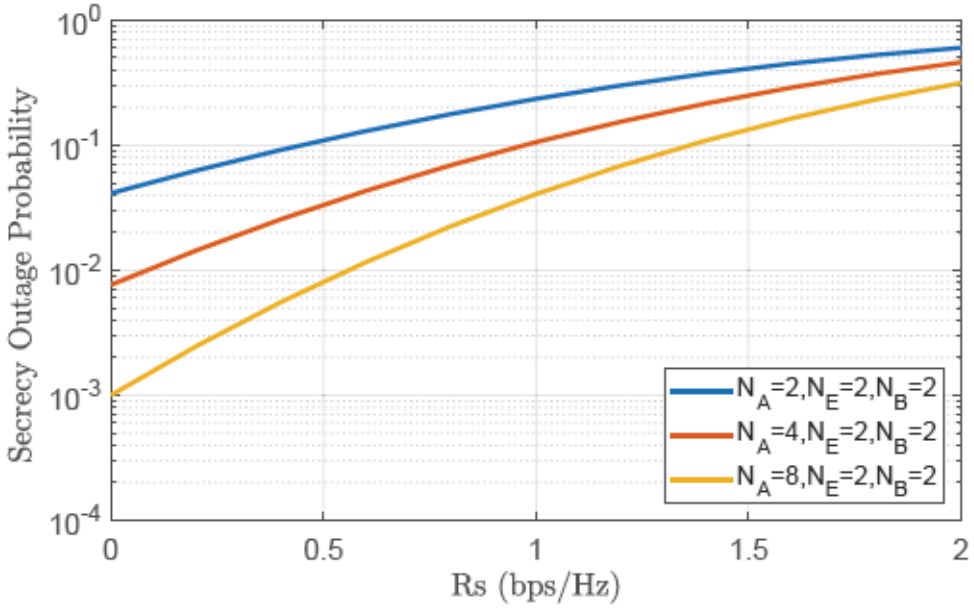

Figure 4.3: Secrecy outage probability as a function of confidential rate R_S

main channel average SNR, $\overline{\gamma}_B$ of 5dB, at a particular secrecy outage probability, secrecy gains as low as 3.5 times and as high as 4.5 times can be achieved by increasing N_A or using a stronger main channel of MIMOME scenario, which confirms the intuition as discuss in Figure 4.8.

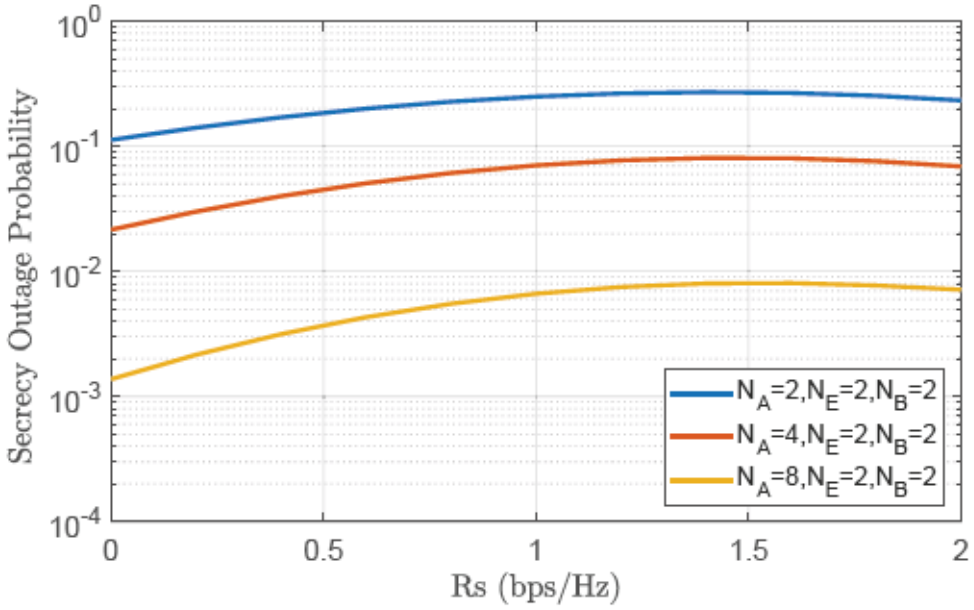

Figure 4.4: Secrecy outage probability as a function of confidential rate R_S

From Figure 4.4, we witnessed that with higher average SNR of legitimate channel i.e., $\overline{\gamma}_B$ of 10 dB, and for an eavesdropper channel with average SNR, $\overline{\gamma}_E$= 0 dB, the secrecy outage probability decrease further as number of antennas at Alice increases, keeping the number of receive antenna at Bob and Eve the same

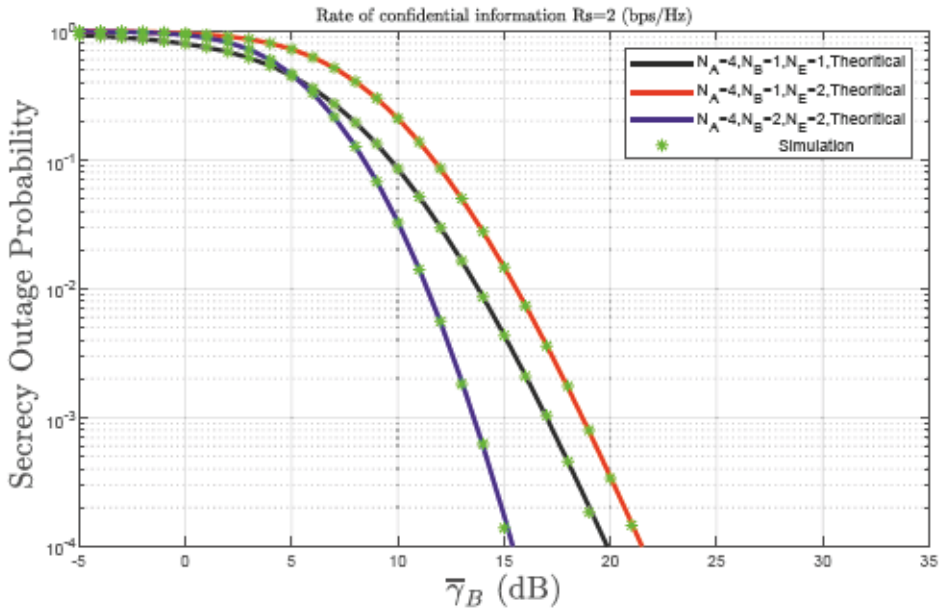

Figure 4.5: Secrecy outage probability as a function of $\overline{\gamma}_B$ for MIMOME scenario

Figure 4.5 represents the secrecy outage probability as a function of $\overline{\gamma}_B$, for three nodes and each node is equipped with multiple antenna, we compare $N_A = 4$, $N_E \in \{1, 2\}$, and $N_B \in \{1, 2\}$, The monte-carlo (MC) simulations results are in agreement

with the closed form expression. In Figure 4.5, we observe that an increase in the N_A causes a decrease in the outage probability while it increases with an increase in the N_E. Therefore our proposed scheme enhances the PHY security even if the eavesdropper is more powerful than Bob.

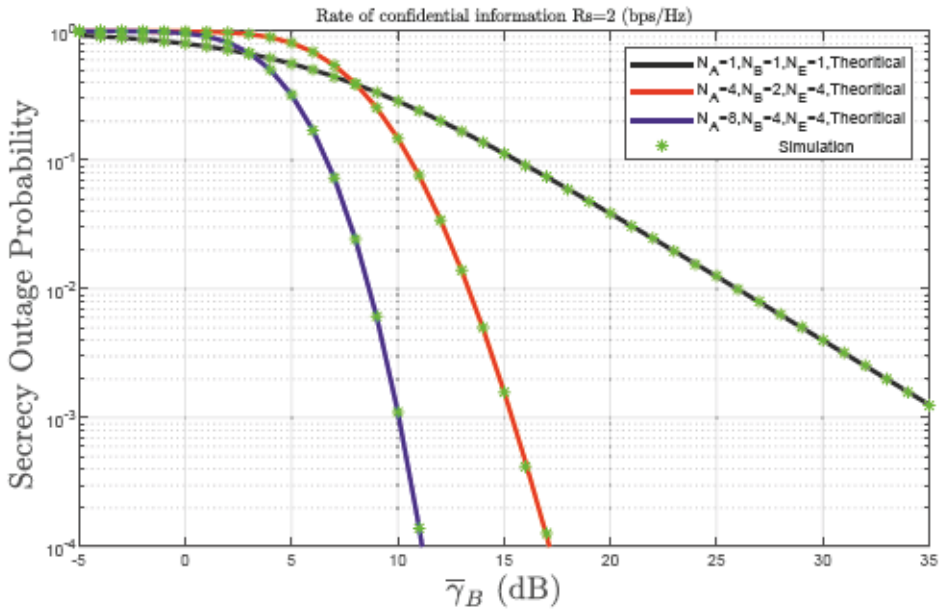

Figure 4.6: Secrecy outage probability as a function of $\overline{\gamma}_B$ for MIMOME scenario

For a fixed secrecy rate $R_S = 2$ bits/s/Hz and $\overline{\gamma}_E$= 0 dB, For $N_A \in \{1, 4, 8\}$, $N_E \in \{1, 4\}$ and $N_B \in \{1, 2, 4\}$ our simulation results show that the presence of multiple antenna at the legitimate transmitter causes an increase in the secrecy outage probability. Furthermore, employing TAS technique does not allow the eavesdropper to exploit transmitter's additional spatial diversity. The monte-carlo simulation corroborates our analytical results.

4.3. Secrecy-Relaibility Trade-off in MIMOME Scenario

In this section, we discuss the secrecy-reliability trade off. The contour plot in Figure 4.7 indicates secrecy outage probability as a function of N_A and N_E. For N_B= 2, average SNR at Bob $\overline{\gamma}_B$= 5 dB and $\overline{\gamma}_E$= 0 dB, secrecy outage probability in MIMOME environment decreases as the number of transmit antenna increases and better security can be achieved. However, secrecy outage probability is directly proportional to the number of the antenna at Eve, which reduces performance.

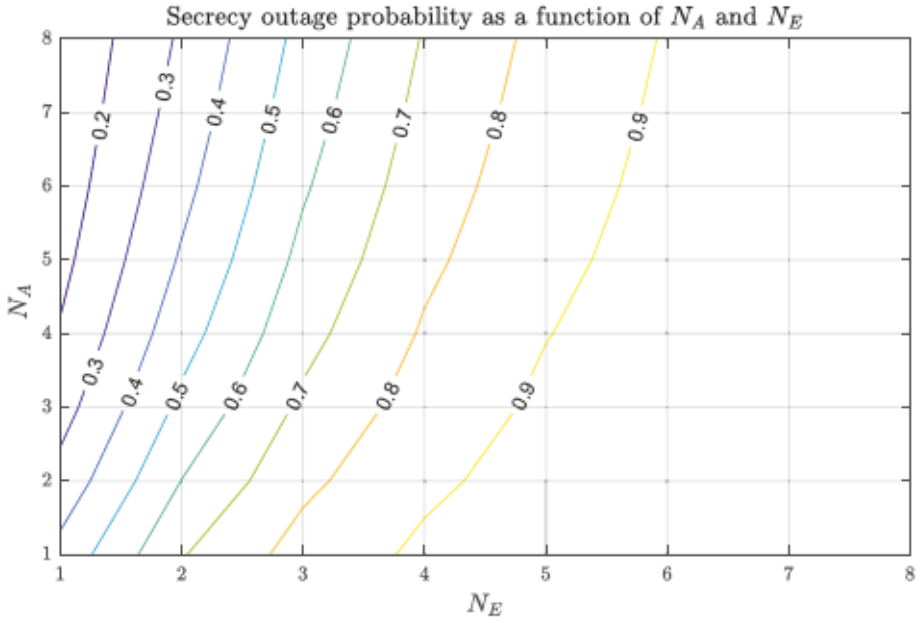

Figure 4.7: Secrecy outage probability as a function of N_A and N_E for MIMOME case

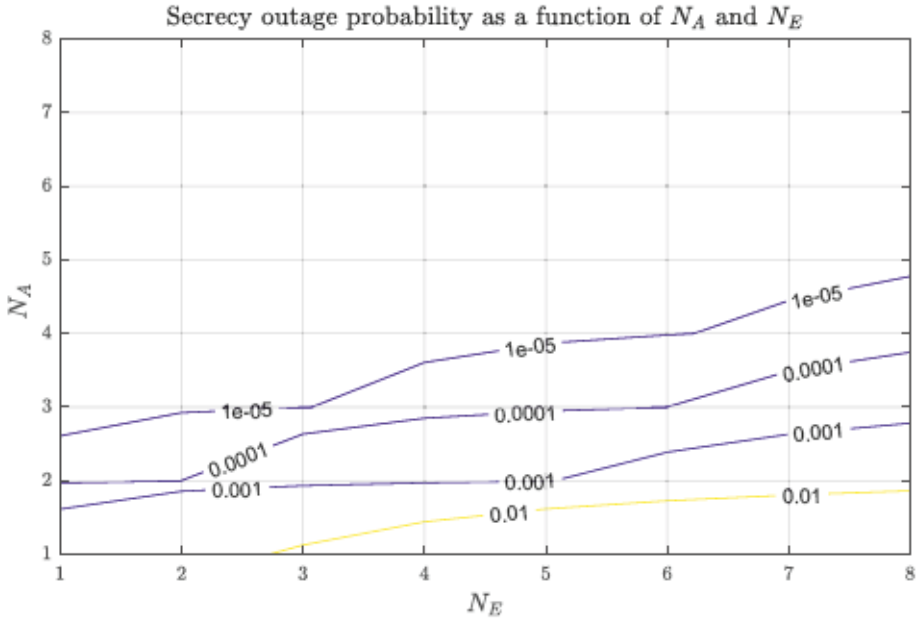

Figure 4.8: Secrecy outage probability as a function of N_A and N_E for MIMOME case

The contour plot in Figure 4.8 represents the secrecy outage probability as function of N_A and N_E for $N_B = 2$, $\overline{\gamma}_B$= 10 dB and $\overline{\gamma}_E = 0$ dB. Notice that by increasing the average SNR ratio between legitimate and eavesdropper channel, it is possible to achieve much lower secrecy outage probability, less than 0.1%, even if Eve has several antennas. Therefore, we can conclude that increasing the power ratio between legitimate and Eve's channel play the crucial role in the performance of the network.

4.4. Secrey-Reliability Assessement under Ultra-Reliable Requirement

We discuss the secrecy-reliability assessement under ultra-reliable requirement. Figure

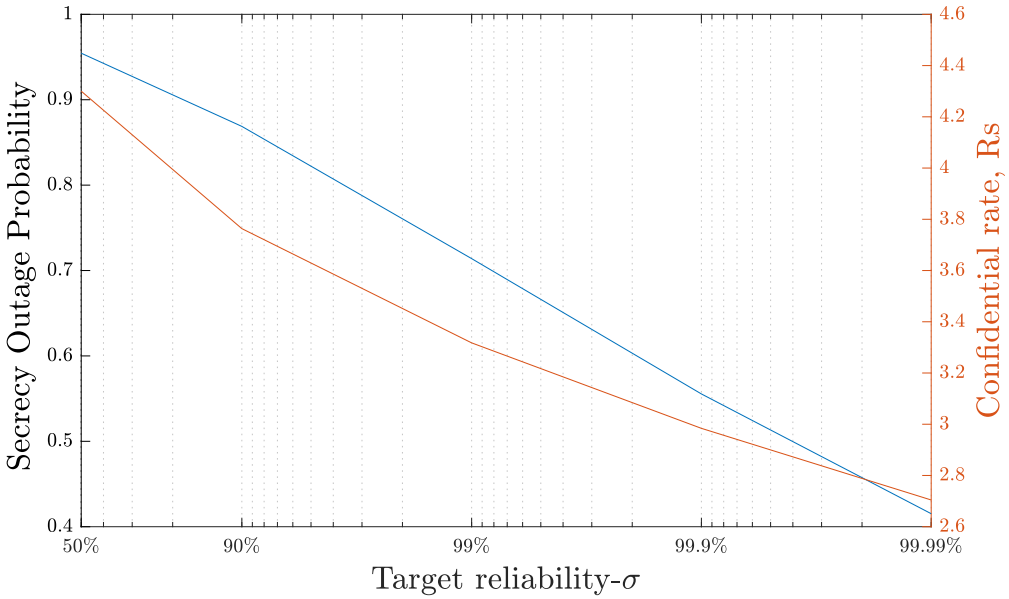

Figure 4.9: Secrecy outage probability as a function of Target Reliability σ

4.9 illustrates the outage secrecy probability as a function of target reliability for N_A = 4, N_E = 2 and N_B = 4 at $\overline{\gamma}_B = 5$ dB and $\overline{\gamma}_E = 0$ dB, For worse case condition where the reliability target is defined as solely based on the secrecy rate, therefore $P_{tx}(Rs, \gamma_B) \geq \sigma$, which after solving it in R_S yields results, the results are put in (32). We evaluate σ, which is considered as a QoS or reliability indicator. Our results show that the system becomes secure as the value of target reliability σ increases, which is a counter-intuitive result once the system is more reliable and secure at the same time. However notice that secure rate R_S is tied to the reliability so that $P_{tx} = \sigma$, which allows for large secure rates that are not optimal and therefore large security outage probability. The rate decreases with an increase in target reliability, but this is not an optimum rate. In fact, this is the worse case scenario as discussed as well in [39]. Thus we aim to perform rate allocation as our future work.

5. CONCLUSION

In this research work, we discuss physical layer security for machine type communication networks due to its high vulnerability to eavesdropping attack. Communication security is one of the basics requirement for 5G and, unusually for IoT and MTC gave their full range of military, industrial and commercial applications. Existing techniques for security are mainly based on cryptography, which works at upper levels of wireless network media with the assumption that eavesdropper has constrained computational capabilities. However, this assumption no longer holds true due to the drastic growth in the computation capabilities of devices. Authentication procedures, maintenance, and distribution of encryption keys are some of the other issues with existing security techniques, In case both parties (transmitter and receiver) do not have such a key or code, another secure channel is needed to share this key or code that requires network resources. Physical layer security as an alternative to cryptography can eradicate the need for encryption keys and is considered more superior for achieving tight security against any level of computational capabilities. Recent developments in the field of Information Theory has resulted in an increased interest in physical level security since it can improve the error probability and confidentiality.

In this work, we considered the multiple wiretap channels where the legitimate pair, Alice (the transmitter) and Bob (the receiver), communicates in the presence of untrusted eavesdropper (Eve) who attempts to breach the transmission originating from Alice. First, we provided a literature review in chapter 2 where we studied the two secrecy outage probability formulations for SISOSE case where all three nodes have a single antenna. The old formulation is given in [27] and in the same article, it was revealed that even if eavesdropper has better average SNR than the legitimate pair, we still have perfectly secure communication. In article [39] the new formulation for secrecy outage probability is derived even if the transmitted message fails to achieve perfect secrecy. In chapter 3 we provided a system model for multiple antennas system to increase the security and reliability of the wireless communication system, this arrangement provides diversity as well as high rate of data transfer because of multiplexing gain. Alice, Bob and Eve all could estimate their own channel state information. Generalized closed-form expressions have been evaluated for the secrecy outage probability of MIMOME while assuming that Alice employs TAS and receivers utilize MRC, for MISOSO only Alice uses TAS, for MIMOSE Alice exploits TAS and Bob resorts to MRC and for MISOME Alice utilizes TAS but only Eve implements MRC. We then provided the numerical analysis of all closed-form expressions introduced. We investigated the behavior of secrecy outage probability as a function of average SNR at Bob $\overline{\gamma}_B$, the rate of confidential information R_S and reliability. We noticed that security is enhanced by the increase in the number of the antennas at Alice and it reduced with an increase in the number of the antennas at Eve. In future, we aim to study rate allocation for the provided closed-form expressions of multiple antenna systems. We will work on traffic models for MTC networks, and the basis for designing and optimization of networks of the future are considered to be the understanding of MTC traffic properties. While doing so, it is pertinent to keep into perspective the relevant QoS schemes and the provision of suitable MTC services for communication without conceding any of the regular HTC services (data, voice, and video).

We also aim to work on covert communication which is a type of communication in which the information transmitted is kept hidden from any potential eavesdropper, i.e., warden. The signals received by the warden must be the same as the ambient signals, i.e., signals received when no transmission is being made. The maximum amount of information which can be covert communicated measures the same as a square root of the total number of channel users. The impact of channel uncertainties on covert communication shows the scenario in which the noise level is random and stays constant during the communication. It is also unknown to the warden, which makes it very difficult for a warden to determine whether the reception it is receiving is signal or noise. Resultantly, favorable covert communication rates are attainable in the absence of unknown noise level supposition. Thus, covert communication is a promising line of research.

6. REFERENCES

[1] P. Pirinen, "A brief overview of 5g research activities," in *1st International Conference on 5G for Ubiquitous Connectivity*, Nov 2014, pp. 17–22.

[2] P. Popovski, V. Braun, H. Mayer, P. Fertl, Z. Ren, D. Gonzales-Serrano, E. Ström, T. Svensson, H. Taoka, P. Agyapong *et al.*, "Scenarios requirements and kpis for 5g mobile and wireless system," *The METIS project: Mobile and wireless communications Enablers for the Twenty-twenty Information Society, Tech. Rep. ICT-317669-METIS D*, vol. 1, 2013.

[3] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, and P. Popovski, "Five disruptive technology directions for 5g," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 74–80, February 2014.

[4] C. Chen, "C-ran: the road towards green radio access network," *White paper*, pp. 2168–7161, 2011.

[5] L. Wei, R. Q. Hu, Y. Qian, and G. Wu, "Key elements to enable millimeter wave communications for 5g wireless systems," *IEEE Wireless Communications*, vol. 21, no. 6, pp. 136–143, December 2014.

[6] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3590–3600, November 2010.

[7] E. G. Larsson, "Massive mimo for 5g: Overview and the road ahead," in *2017 51st Annual Conference on Information Sciences and Systems (CISS)*, March 2017, pp. 1–1.

[8] P. Popovski, "Ultra-reliable communication in 5g wireless systems," in *1st International Conference on 5G for Ubiquitous Connectivity*, Nov 2014, pp. 146–151.

[9] J. G. Andrews, "Seven ways that hetnets are a cellular paradigm shift," *IEEE Communications Magazine*, vol. 51, no. 3, pp. 136–144, March 2013.

[10] P. Popovski, J. J. Nielsen, C. Stefanovic, E. d. Carvalho, E. Strom, K. F. Trillingsgaard, A. S. Bana, D. M. Kim, R. Kotaba, J. Park, and R. B. Sorensen, "Wireless access for ultra-reliable low-latency communication: Principles and building blocks," *IEEE Network*, vol. 32, no. 2, pp. 16–23, March 2018.

[11] M. Bennis, M. Debbah, and H. V. Poor, "Ultra-reliable and low-latency wireless communication: Tail, risk and scale," *arXiv preprint arXiv:1801.01270*, 2018.

[12] C.-P. Li, J. Jiang, W. Chen, T. Ji, and J. Smee, "5g ultra-reliable and low-latency systems design," in *2017 European Conference on Networks and Communications (EuCNC)*, June 2017, pp. 1–5.

[13] E. Zeydan, E. Bastug, M. Bennis, M. A. Kader, I. A. Karatepe, A. S. Er, and M. Debbah, "Big data caching for networking: moving from cloud to edge," *IEEE Communications Magazine*, vol. 54, no. 9, pp. 36–42, September 2016.

[14] E. Bastug, M. Bennis, and M. Debbah, "Living on the edge: The role of proactive caching in 5g wireless networks," *IEEE Communications Magazine*, vol. 52, no. 8, pp. 82–89, Aug 2014.

[15] J. Konečnỳ, H. B. McMahan, D. Ramage, and P. Richtárik, "Federated optimization: Distributed machine learning for on-device intelligence," *arXiv preprint arXiv:1610.02527*, 2016.

[16] P. Popovski, J. J. Nielsen, C. Stefanovic, E. d. Carvalho, E. Strom, K. F. Trillingsgaard, A. S. Bana, D. M. Kim, R. Kotaba, J. Park, and R. B. Sorensen, "Wireless access for ultra-reliable low-latency communication: Principles and building blocks," *IEEE Network*, vol. 32, no. 2, pp. 16–23, March 2018.

[17] O. L. A. López, H. Alves, P. H. J. Nardelli, and M. Latva-aho, "Aggregation and resource scheduling in machine-type communication networks: A stochastic geometry approach," *IEEE Transactions on Wireless Communications*, vol. 17, no. 7, pp. 4750–4765, July 2018.

[18] O. L. A. Lopez, H. Alves, and M. Latva-aho, "Rate control under finite blocklength for downlink cellular networks with reliability constraints," *arXiv preprint arXiv:1806.04386*, 2018.

[19] M. Vural, P. Jung, and S. Stanczak, "On some physical layer design aspects for machine type communication," in *WSA 2016; 20th International ITG Workshop on Smart Antennas*, March 2016, pp. 1–8.

[20] Z. Dawy, W. Saad, A. Ghosh, J. G. Andrews, and E. Yaacoub, "Toward massive machine type cellular communications," *IEEE Wireless Communications*, vol. 24, no. 1, pp. 120–128, February 2017.

[21] 3GPP, "Technical specification groups radio access network; evolved universal terrestrial radio access (e-utra); user equipment (ue) conformance specification radio transmission and reception," 3GPP, Tech. Rep. TS 36.104 version 9.4.0 Release 9, july 2010.

[22] R. Ratasuk, A. Prasad, Z. Li, A. Ghosh, and M. A. Uusitalo, "Recent advancements in m2m communications in 4g networks and evolution towards 5g," in *Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on*. IEEE, 2015, pp. 52–57.

[23] N. Brahmi and V. Venkatasubramanian, "Mobile and wireless communications enablers for the twenty-twenty information society (metis)," *Tech. Rep.*, 2013.

[24] P. Bhat and M. Dohler, "Overview of 3gpp machine-type communication standardization," in *Machine-to-machine (M2M) Communications*. Elsevier, 2015, pp. 47–62.

[25] T. Grgic and M. Matijasevic, "Performance metrics for context-based charging in 3gpp online charging system," in *Proceedings of the 12th International Conference on Telecommunications*, June 2013, pp. 171–178.

[26] M. Laner, N. Nikaein, P. Svoboda, M. Popovic, D. Drajic, and S. Krco, "Traffic models for machine-to-machine (m2m) communications: types and applications," in *Machine-to-machine (M2M) Communications*. Elsevier, 2015, pp. 133–154.

[27] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *2006 IEEE International Symposium on Information Theory*, July 2006, pp. 356–360.

[28] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[29] A. O. Hero, "Secure space-time communication," *IEEE Transactions on Information Theory*, vol. 49, no. 12, pp. 3235–3249, 2003.

[30] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. McLaughlin, and J.-M. Merolla, "Capacity achieving codes for the wiretap channel with applications to quantum key distribution," *arXiv preprint cs.IT/0411003*, vol. 1, 2004.

[31] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J. m. Merolla, "Ldpc-based secret key agreement over the gaussian wiretap channel," in *2006 IEEE International Symposium on Information Theory*, July 2006, pp. 1179–1183.

[32] Y.-F. Huang and H. H. Chen, "Physical layer architectures for machine type communication networks-a survey," *Wireless Communications and Mobile Computing*, vol. 16, no. 18, pp. 3269–3294, 2016.

[33] M. Chen, J. Wan, S. Gonzalez, X. Liao, and V. C. M. Leung, "A survey of recent developments in home m2m networks," *IEEE Communications Surveys Tutorials*, vol. 16, no. 1, pp. 98–114, First 2014.

[34] E.-K. Lee, M. Gerla, and S. Y. Oh, "Physical layer security in wireless smart grid," *IEEE Communications Magazine*, vol. 50, no. 8, 2012.

[35] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE wireless Communications*, vol. 18, no. 2, 2011.

[36] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[37] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[38] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE transactions on information theory*, vol. 24, no. 4, pp. 451–456, 1978.

[39] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Communications Letters*, vol. 15, no. 3, pp. 302–304, March 2011.

[40] P. Parada and R. Blahut, "Secrecy capacity of simo and slow fading channels," in *Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on*. IEEE, 2005, pp. 2152–2155.

[41] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Friendly jamming for wireless secrecy," in *Communications (ICC), 2010 IEEE International Conference on*. IEEE, 2010, pp. 1–6.

[42] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure hybrid-arq protocols for gaussian block-fading channels," *IEEE Transactions on Information Theory*, vol. 55, no. 4, pp. 1575–1591, April 2009.

[43] H. Alves, R. D. Souza, and M. Debbah, "Enhanced physical layer security through transmit antenna selection," in *2011 IEEE GLOBECOM Workshops (GC Wkshps)*, Dec 2011, pp. 879–883.

[44] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Processing Letters*, vol. 19, no. 6, pp. 372–375, June 2012.

[45] X. Tang, R. Liu, and P. Spasojevic, "On the achievable secrecy throughput of block fading channels with no channel state information at transmitter," in *Information Sciences and Systems, 2007. CISS'07. 41st Annual Conference on*. IEEE, 2007, pp. 917–922.

[46] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure hybrid-arq protocols for gaussian block-fading channels," *IEEE Transactions on Information Theory*, vol. 55, no. 4, pp. 1575–1591, 2009.

[47] H. Alves, M. D. CastroTomé, P. H. J. Nardelli, C. H. M. D. Lima, and M. Latva-Aho, "Enhanced transmit antenna selection scheme for secure throughput maximization without csi at the transmitter," *IEEE Access*, vol. 4, pp. 4861–4873, 2016.

[48] M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions: with formulas, graphs, and mathematical tables*. Courier Corporation, 1964, vol. 55.